nedelja informatike 3

Kvantno računarstvo

Marina Ivanović

Matematička gimnazija
Nedelja informatike[3]

15. decembar 2016.

Uvod u predavanje

- Šta je to kvantno računarstvo?
  - Oblast računarstva koja koristi fenomene kvantne fizike.
- Zašto se baviti kvantnim računarstvom?
  - Svet je kvantan.
  - Uređaji su sve manji.
  - Mogu nam doneti nešto do sad nemoguće.

O čemu ćemo pričati?

- Superpozicija - Bits & Qbits
- Matematički model
- Kvantna kola
- Algoritmi
  - Quantum Cryptography
  - Quantum Teleportation
  - Quantum Search

Bitovi

- Bacivši novčić - *ili* glava *ili* pismo.
- Glava $\rightarrow 0$, pismo $\rightarrow 1$, ovo možemo posmatrati kao bit koji može biti *ili* 0 *ili* 1.
- Verovatnoća da je bačena glava g, a da je bačeno pismo p, s tim da važi $g + p = 1$.
- Stanje sistema matrično prikazano

$$g \begin{bmatrix} 1 \\ 0 \end{bmatrix} + p \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} g \\ p \end{bmatrix}$$

- Nakon merenja biće dobijena 0 (glava) sa verovatnoćom g ili 1 (pismo) sa verovatnoćom p.
- g i p su realni brojevi.

Qubiti

- Bacivši novčić - *i* glava *i* pismo, do merenja!
- Glava $\rightarrow 0$, pismo $\rightarrow 1$, ovo možemo posmatrati kao qubit koji je *i* 0 *i* 1.
- Stanje sistema matrično prikazano kao vektor verovatnoće

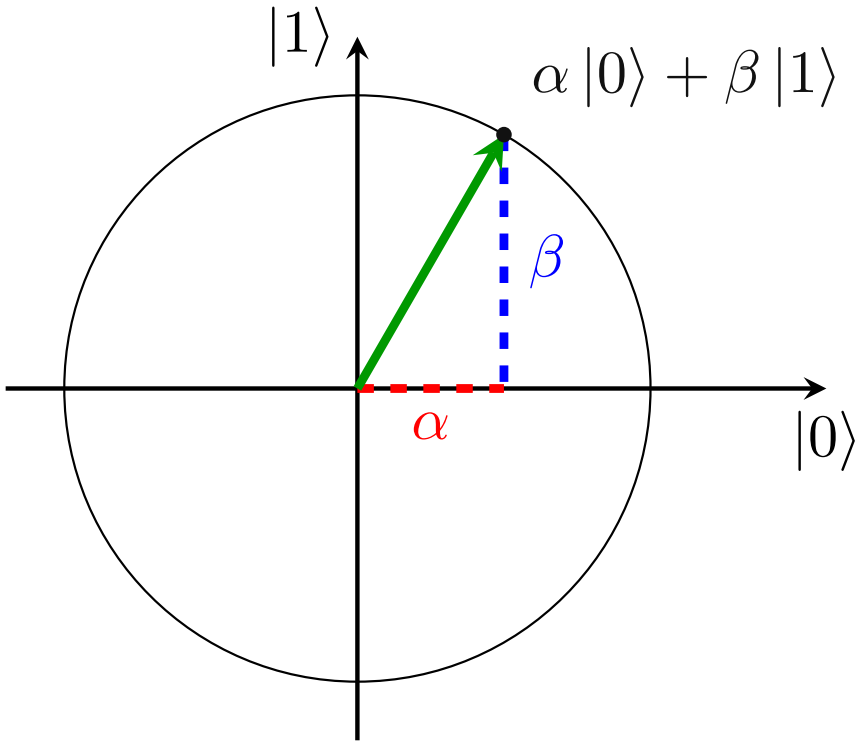
$$\alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

- Nakon merenja biće dobijena 0 (glava) sa verovatnoćom $|\alpha|^2$ ili 1 (pismo) sa verovatnoćom $|\beta|^2$, pritom važi $|\alpha|^2 + |\beta|^2 = 1$.
- α i β mogu biti kompleksni brojevi!

ket notacija

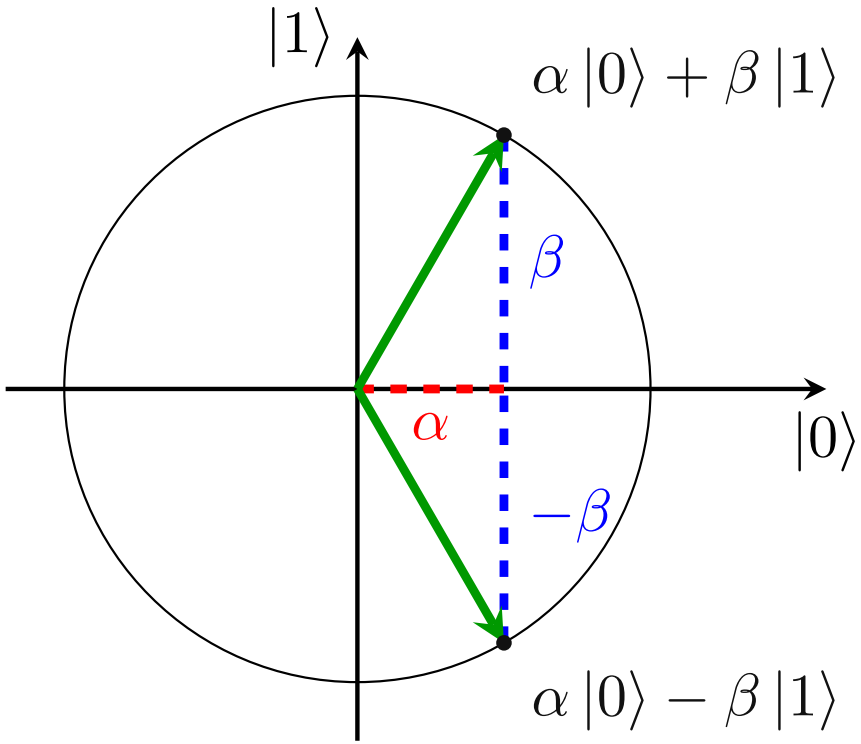
- $\begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$
- $\begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$
- $\alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha |0\rangle + \beta |1\rangle$

Geometrijska interpretacija



- Iz svakog qubita se može dobiti tačno jedan bit informacije nakon merenja.
- Nakon merenja, sistem prelazi u izmereno stanje.
- Svaki sledeći put nakon merenja će se dobiti isti rezultat.

Primer



- $\alpha|0\rangle + \beta|1\rangle$ i $\alpha|0\rangle - \beta|1\rangle$ imaju iste verovatnoće merenja 0 odnosno 1.
- Ipak, ovo su različita stanja i drugačije se ponašaju!

n-qubit

- (Matrična) predstava ket notacijom n qubita.
- Primer: $|000\rangle$ - 3-qubit, gde su u ovom primeru svi 0.
- $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

Entanglement

- 2 qubita su entanglovana (uvezana, upletena) ako *merenje jednog utiče na drugog*.

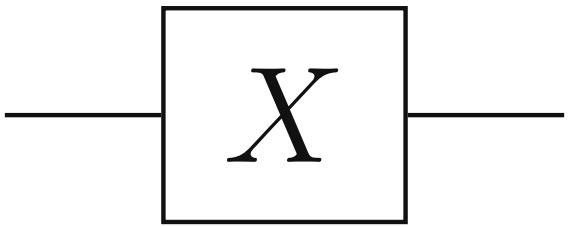
- $\frac{1}{\sqrt{2}} \cdot (|01\rangle + |10\rangle)$

- Entanglovani qubiti se ne mogu napisati u *odvojenim stanjima*.

Belova stanja

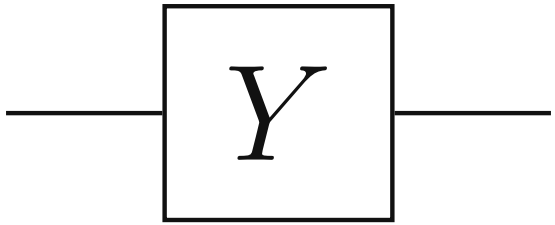
- $\frac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle)$
- $\frac{1}{\sqrt{2}} \cdot (|01\rangle + |10\rangle)$
- $\frac{1}{\sqrt{2}} \cdot (|00\rangle - |11\rangle)$
- $\frac{1}{\sqrt{2}} \cdot (|01\rangle - |10\rangle)$

Pauli gate X



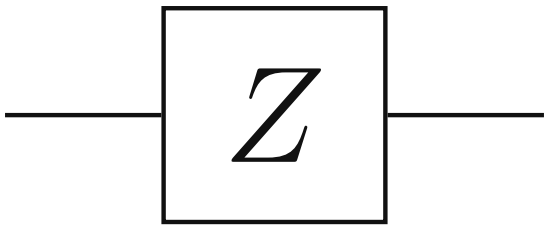
- $X|0\rangle = |1\rangle$
- $X|1\rangle = |0\rangle$
- $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Pauli gate Y



- $Y|0\rangle = i|1\rangle$
- $Y|1\rangle = -i|0\rangle$
- $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

Pauli gate Z

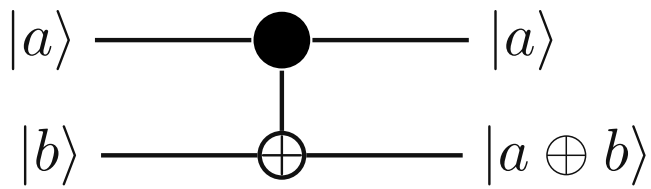


- $Z|0\rangle = |0\rangle$
- $Z|1\rangle = -|1\rangle$
- $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Hadamard gate

- $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

Controlled Not



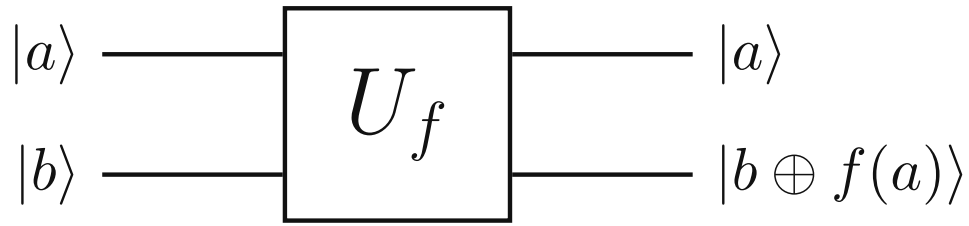
- Menja drugi qubit ako je prvi 1, inače ga ne menja.

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

Deutsch-Jozsa Problem

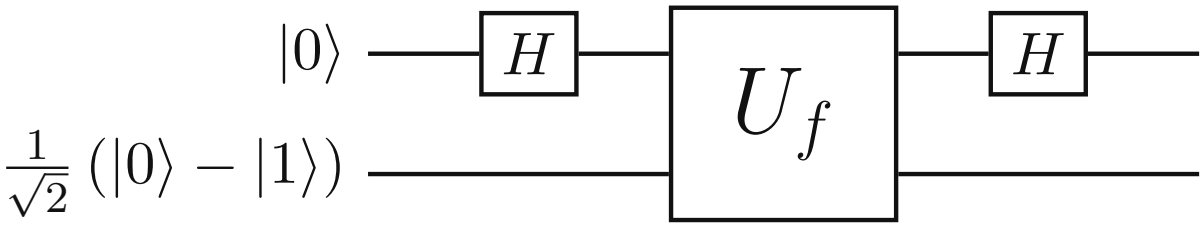
- $f : \{0, 1\} \to \{0, 1\}$
- Kakva je ova funkcija?
  - balansirana - $f(0) \neq f(1)$
  - konstantna - $f(0) = f(1)$
- Koliko je merenja potrebno da bismo to saznali?
  - klasično računarstvo - 2
  - kvantno računarstvo - 1

Kvantna crna kutija *Uf*



- Šta se desi kada U_f primenimo dva puta?
  - $|a\rangle \rightarrow |a\rangle \rightarrow |a\rangle$
  - $|b\rangle \rightarrow |b \oplus f(a)\rangle \rightarrow |b\rangle$

Algoritam



- Ulaz u U_f
  - $|a\rangle \otimes |b\rangle = (|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) = |00\rangle - |01\rangle + |10\rangle - |11\rangle$
- Izlaz iz U_f
  - $1 \otimes f(x) = not(f(x)) = f^{'}(x)$
  - $|0f(0)\rangle - \left|0f^{'}(0)\right\rangle + |1f(1)\rangle - \left|1f^{'}(1)\right\rangle$

Merenje

- Krajnji izlaz
  - $|0f(0)\rangle + |1f(0)\rangle - \left|0f'(0)\right\rangle - \left|1f'(0)\right\rangle + |0f(1)\rangle - |1f(1)\rangle - \left|0f'(1)\right\rangle + \left|1f'(1)\right\rangle$
- $f(0) = f(1)$
  - $|0f(0)\rangle + |1f(0)\rangle - \left|0f'(0)\right\rangle - \left|1f'(0)\right\rangle + |0f(1)\rangle - |1f(1)\rangle - \left|0f'(1)\right\rangle + \left|1f'(1)\right\rangle = |0f(0)\rangle - \left|0f'(0)\right\rangle =$
    $|0\rangle \otimes (|f(0)\rangle - \left|f'(0)\right\rangle)$
- $f(0) \neq f(1)$
  - $|0f(0)\rangle + |1f(0)\rangle - \left|0f'(0)\right\rangle - \left|1f'(0)\right\rangle + |0f(1)\rangle - |1f(1)\rangle - \left|0f'(1)\right\rangle + \left|1f'(1)\right\rangle = |1f(0)\rangle - \left|1f'(0)\right\rangle =$
    $|1\rangle \otimes (|f(0)\rangle - \left|f'(0)\right\rangle)$

Pretpostavke

- Alice šalje Bobu, Eve prisluškuje.
- Definisanje ključa.
- Alice prenosi niz bitova pomoću qubita.

Protokol

- Alice nasumično bira u kojoj bazi šalje.
- Bob nasumično bira u kojoj bazi prima.
- Bob kaže koje je baze koristio.
- Alice kaže koje su mu bile tačne.
- Od tačnog se pravi ključ, netačno se odbacuje.

Napadi

- Zašto Bob ne sačuva sve poslate qubite, pa onda objaviti u kojem bazisu treba meriti?
  - Bob ih ne može čuvati. Da može, mogla bi i Eve.
- Šta ako Eve presretne qubite i izmeri u nasumičnom bazisu?
  - Onda će ih promeniti. Verovatnoća da je loše izmereno je $\frac{1}{4}$ (pogrešan bazis, pogrešno izmereno). Dovoljno je izabrati proizvoljan broj bitova i proveriti da li se poklapaju (za n bitova dovoljno je da $(\frac{1}{4})^n$ bude dosta mala verovatnoća).
- Šta ako Eve presretne qubite i kopira ih?
  - Ne može! Teorema o kloniranju!

Šta nije teleportacija?

- Saznati šta je ono što želimo da prenesemo.
- Napraviti ga identičnim na drugom mestu.
- Gubljenje karakteristika! Teorema o kloniranju!

Šta jeste teleportacija?

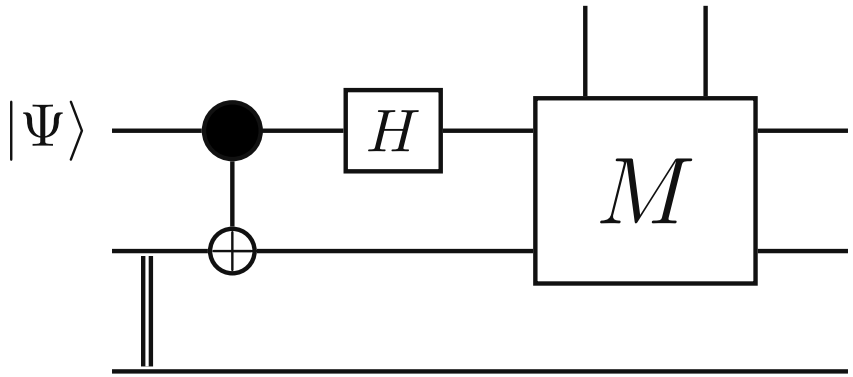
- Preneti informaciju o nečemu bez saznanja šta je to tačno.
- Ne napraviti ga na drugom mestu, već preneti njegove karakteristike.
- *Preneti jedan qubit korišćenjem 2 bita.*

Kvantno kolo

- $|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$
- $|A\rangle$ i $|B\rangle$ su entanglovani, tako da su u stanju

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- Cilj je da važi: $|B\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$



Rezultat

- Ulaz u kolo
  - $|\Psi\rangle \otimes (\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)) = (\alpha|0\rangle + \beta|1\rangle) \otimes (\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)) = \frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\beta}{\sqrt{2}}|100\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|111\rangle$
- Nakon *XOR-a*
  - $\frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\beta}{\sqrt{2}}|110\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|101\rangle$
- Nakon *H*
  - $\frac{\alpha}{2}(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \frac{\beta}{2}(|010\rangle + |001\rangle - |110\rangle - |101\rangle)$

Merenje

- $\frac{\alpha}{2}(|000\rangle+|011\rangle+|100\rangle+|111\rangle)+\frac{\beta}{2}(|010\rangle+|001\rangle-|110\rangle-|101\rangle)$
- 00

$$|B\rangle = I\,|B\rangle = I(\alpha\,|0\rangle + \beta\,|1\rangle) = \alpha\,|0\rangle + \beta\,|1\rangle$$

- 01

$$|B\rangle = X\,|B\rangle = X(\alpha\,|1\rangle + \beta\,|0\rangle) = \alpha\,|0\rangle + \beta\,|1\rangle$$

- 10

$$|B\rangle = Z\,|B\rangle = Z(\alpha\,|0\rangle - \beta\,|1\rangle) = \alpha\,|0\rangle + \beta\,|1\rangle$$

- 11

$$|B\rangle = XZ\,|B\rangle = XZ(\alpha\,|1\rangle - \beta\,|0\rangle) = \alpha\,|0\rangle + \beta\,|1\rangle$$

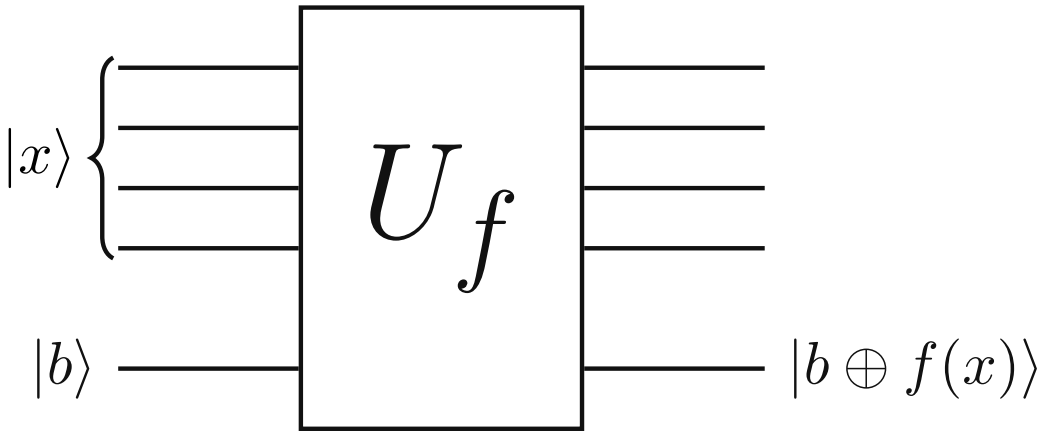
Algoritmi pretrage

- Klasično računarstvo
  - Sortiran niz
  - Binarna pretraga
  - $O(\log N)$
- Kvantno računarstvo
  - Nesortiran niz
  - Groverov algoritam
  - $O(\sqrt{N})$

Niz koji se pretražuje

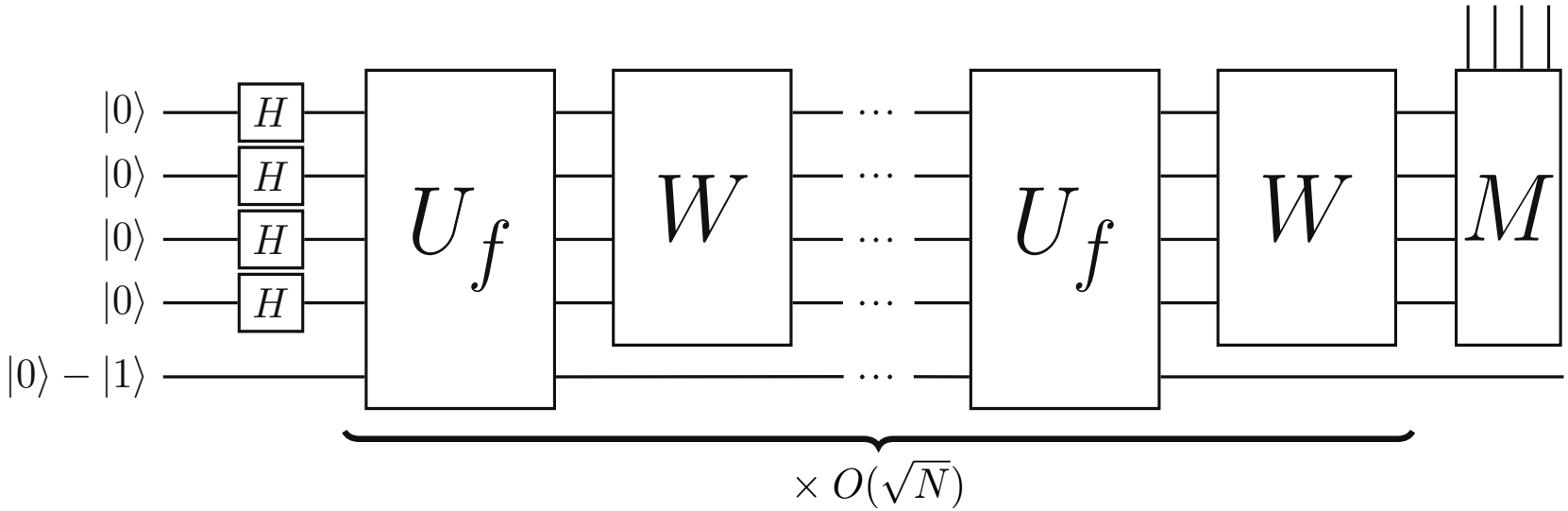
- Neka u nizu ima N elemenata.
- Neka je $N = 2^n$.
- Indeks svakog od elemenata možemo predstaviti binarno uz pomoć n bitova.
- Pretpostavimo da tražimo element koji ima indeks a u binarnom zapisu.

Crna kutija



- Neka je $f : N \to \{0, 1\}$, odnosno funkcija koja operiše nad n bitova.
- Vrednosti funkcije
  - $f(a) = 1$
  - $f(x) = 0, x \neq a$

Algoritam



- Ulaz u kolo je superpozicija svih indeksa koji bi se nakon merenja dobili sa jednakim verovatnoćama, i to $\frac{1}{N}$.
- Ideja Groverovog algoritma: određenim operacijama podići verovatnoću dobijanja indeksa a nakon merenja.

Rezultat operatora U_f

- Izlaz iz U_f
  - $|a\rangle \rightarrow -|a\rangle$
  - $|x\rangle \rightarrow |x\rangle\,, x \neq a$

- Nije nam bitno šta se dešava sa poslednjim qubitom ulaza, pa možemo posmatrati samo transformacije koje se dešavaju na prvih n qubita.

- Neka je V *deo* crne kutije U_f, i to operator nad prvih n qubita.

- $V = I - 2\,|a\rangle\,\langle a|$

Operatori W i G

- Početno ulazno stanje (superpozicija svih indeksa)

$$|\Psi\rangle = H^{\otimes n} |0^n\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle$$

- $W = 2 |\Psi\rangle \langle\Psi| - I$
- Groverov algoritam se sastoji iz ponavljanja $\sqrt{N}$ puta *Groverovog iteratora* G.
- $G = WV = (2 |\Psi\rangle \langle\Psi| - I)(I - 2 |a\rangle \langle a|)$

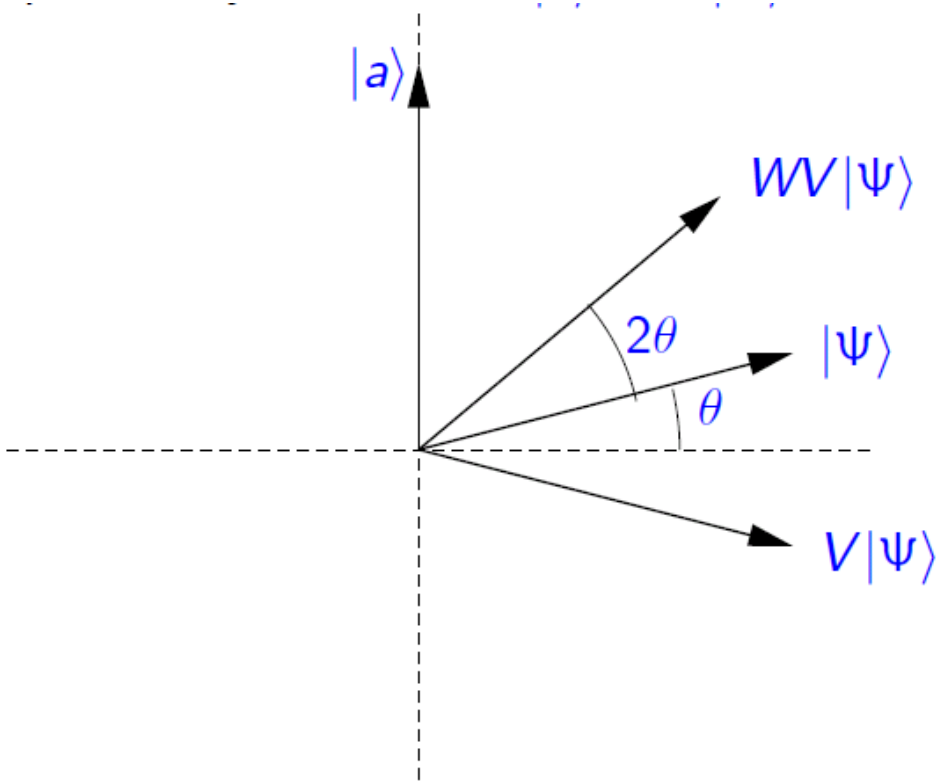
Kako zapravo izgleda W?

- $W = 2\left|\Psi\right\rangle\left\langle\Psi\right| - I$

$$\left|\Psi\right\rangle\left\langle\Psi\right| = \Psi\Psi^{*T} = \begin{bmatrix} \frac{1}{\sqrt{N}} \\ \cdot \\ \cdot \\ \frac{1}{\sqrt{N}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{N}} & \cdot & \cdot & \frac{1}{\sqrt{N}} \end{bmatrix}$$

$$= \begin{bmatrix} \frac{1}{N} & \cdot & \cdot & \frac{1}{N} \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ \frac{1}{N} & \cdot & \cdot & \frac{1}{N} \end{bmatrix}$$

Geometrijska interpretacija



- V je simetrija oko normale na $|a\rangle$.
- W je simetrija oko $|\Psi\rangle$.
- Kompozicija dve simetrije je *rotacija*.

Zašto iteracije ponoviti baš $\sqrt{N}$ puta?

- Nakon svake iteracije $|\Psi\rangle$ se zarotira za 2θ približivši se $|a\rangle$.
- Za veliko N možemo reći da su $|a\rangle$ i $|\Psi\rangle$ *ortogonalni*, tj. da je ugao između njih $\frac{\pi}{2}$.
- Tada važi

$$\theta \sim \sin\theta = \langle a|\Psi\rangle = \frac{1}{\sqrt{N}}.$$

- Nakon $t \sim \frac{\frac{\pi}{2}}{2\theta} \sim \frac{\pi}{4}\frac{1}{\theta} \sim \frac{\pi}{4}\sqrt{N}$ iteracija, stanje sistema će biti

$$G^t |\Psi\rangle,$$

  i to na ugao θ od $|a\rangle$.
- $|a\rangle$ će biti izmereno sa verovatnoćom

$$\left|\langle G^t\Psi|a\rangle\right|^2 \geq \cos^2\theta = 1 - \sin^2\theta = \frac{N-1}{N}.$$

O čemu smo danas pričali?

- Šta su kvantno računarstvo i qubiti.
- Kako izgleda matematički model koji se koristi u kvantnom računarstvu.
- Nekoliko jednostavnih kvantnih kola.
- Kriptografija - definisanje ključa za dekodiranje.
- Teleportacija - preneti jedan qubit uz pomoć dva bita.
- Groverov algoritam - povećanje verovatnoće dobijanja traženog elementa nesortiranog niza u $O(\sqrt{N})$.

Hvala na pažnji!

- Da li iko razume kvantno računarstvo?
  - $\frac{1}{\sqrt{2}}(|da\rangle + |ne\rangle)$