Kvantno računanje

Uvod: • Listopad 2019, **kvantna premoć**

Googlovo računalo Syncamore (54 qubita)
200 sec v.s. 10 000 godina
(2.5 dana?)

• ideja o računanju baziranom na zakonima kvantne mehanike je još iz 70'; Benioff, Feynman, Deutch

• 1994 **Peter Shor** - efikasan algoritam za faktorizaciju
- problem diskretnog logaritma

sigurnost moderne kriptografije je bazirana na ova dva problema

- kvantna računala danas: 100ak qubita, nema zanimljivih primjena
  - za faktorizaciju u kriptografiji: 20 milijuna qubita

- jedna od prvih primjena će biti u simulacijama kemijskih reakcija

- IBM Q (kvantno računalo u oblaku)
  i vi možete isprobati (qiskit)

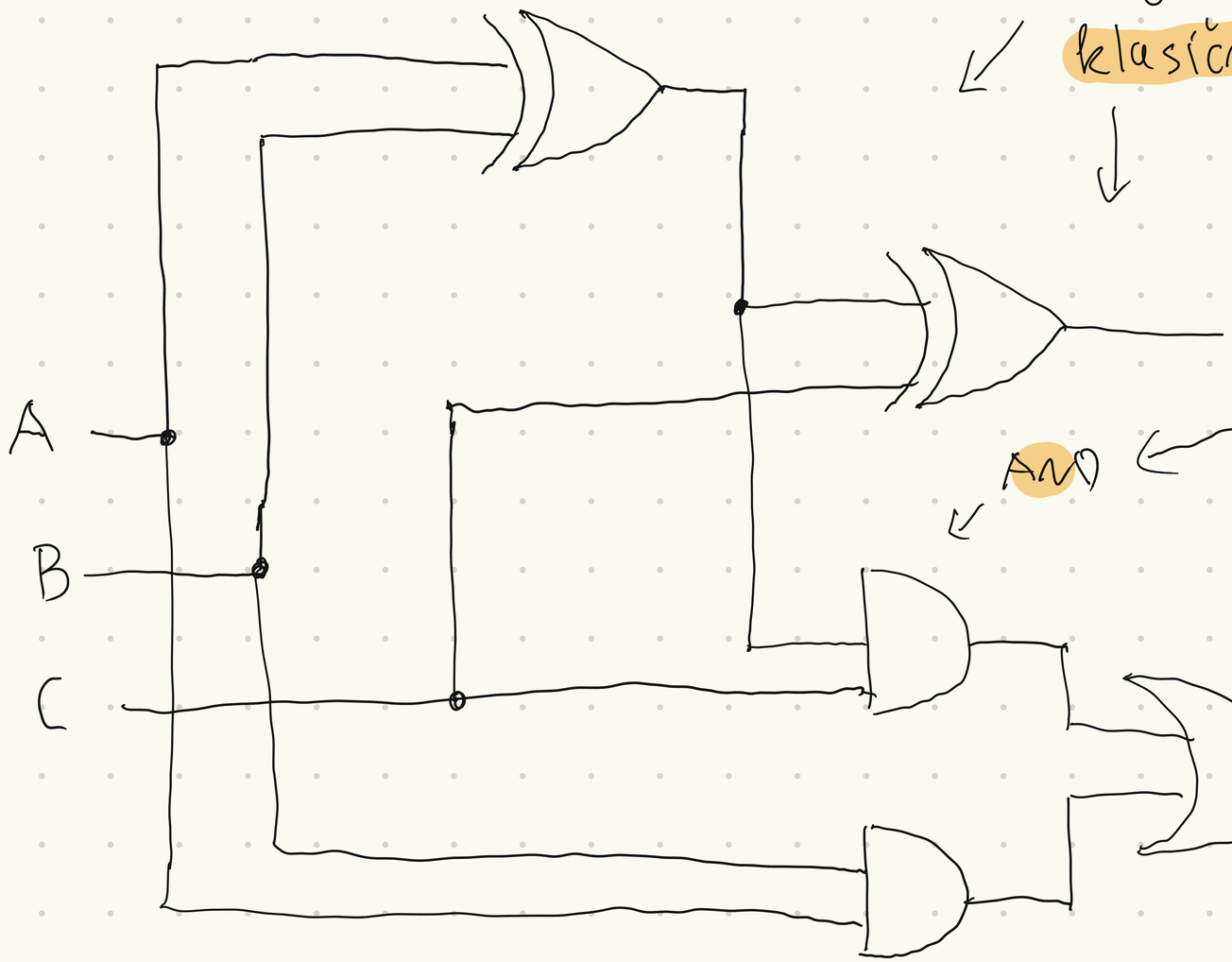
Bit v.s. qubit

XOR

logični sklop

klasično računanje

seštevalo



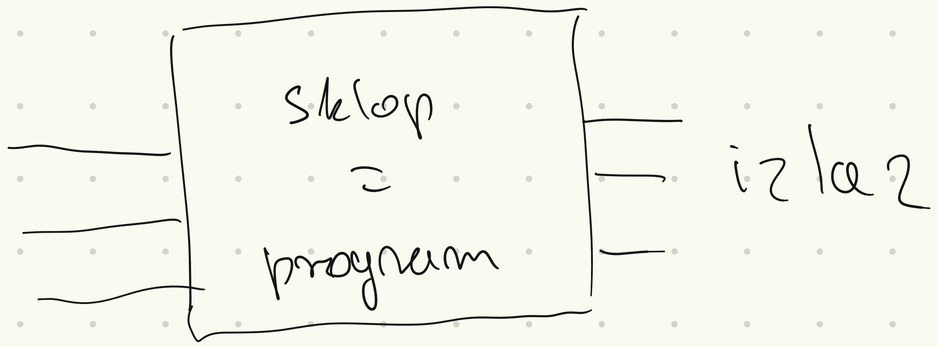
suma = A+B+C mod 2

AND

logična vrata

OR

"jeclam clalja"

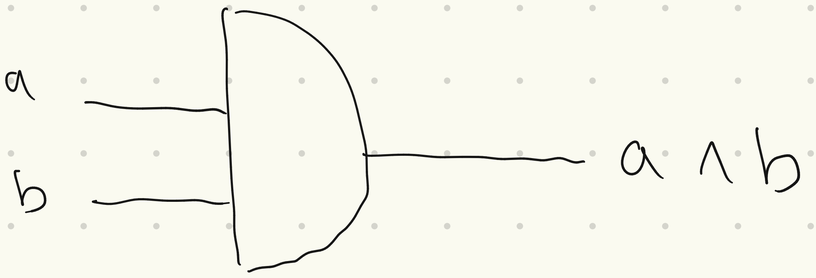


unos

izlaz

bit ——— dva stanja 0 ili 1

logička vrata



qubit ... zbunjujuće, stanje qubita je **superpozicija** stanja $|0\rangle$ i $|1\rangle$

pišemo: $a|0\rangle + b|1\rangle$ gdje su $a, b \in \mathbb{C}$ t.d. $|a|^2 + |b|^2 = 1$

$(a, b) \in \mathbb{C}^2$

vektor

kompleksni brojevi

no kad želimo očitati stanje qubita (**mjerenje**) qubit će se nalaziti u stanju $|0\rangle$ ili $|1\rangle$!

vjerojatnost: • ako bacimo kocku, vjerojatnost da ćemo dobiti šesticu je $\frac{1}{6} \approx 16.7\%$

• ako očitamo (izmjerimo) qubit koji se nalazi u stanju $a|0\rangle + b|1\rangle$, vjerojatnost da ćemo dobiti $|0\rangle$ je $|a|^2$ (dok je vjerojatnost za $|1\rangle$ jednaka $1 - |a|^2 = |b|^2$)

• zbog ovog svojstva qubita svi kvantni algoritmi su **vjerojatnosni**

kvantna vrata (koja djeluju na jedan qubit)

(unitarni) linearni operatori nu $\mathbb{C}^2$

$a|0\rangle + b|1\rangle$ — X — $b|0\rangle + a|1\rangle$

$a|0\rangle + b|1\rangle$ — Z — $a|0\rangle - b|1\rangle$

Hadamardova vrata

$a|0\rangle + b|1\rangle$ — H — $a \cdot \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + b \cdot \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Što ako imamo više od jednog qubita?

3 bita mogu biti u jednom od 8 stanja

000
001
010
011
100
101
110
111

sustav od 3 qubita se opisuje superpozicijom

$$a_0|000\rangle + a_1|001\rangle + a_2|010\rangle + \dots + a_7|111\rangle$$

gdje su $a_i \in \mathbb{C}$ t.d. $\sum_{i=0}^{7} |a_i|^2 = 1$

Stanja možemo "množiti":

ako se 1. qubit nalazi u stanju $a|0\rangle + b|1\rangle$, a drugi u stanju $c|0\rangle + d|1\rangle$, onda sustav od ta dva qubita opisujemo produktom

množimo svaki sa svakim s time da $|0\rangle|1\rangle \neq |1\rangle|0\rangle$

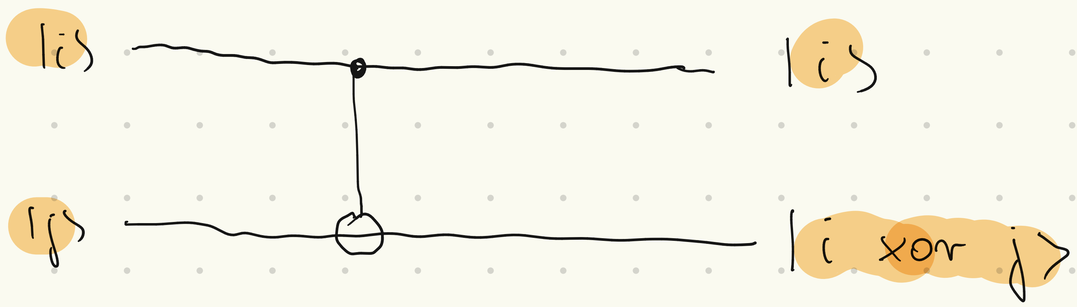
$\|$ $\|$

$|01\rangle$ $|10\rangle$

$$(a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle) = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$$

(Uočite $|ac|^2 + |ad|^2 + |bc|^2 + |bd|^2 = 1$)

CNOT operator (djeluje na dva qubita)



djelovanje na bazi $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ (unitarnog operatora)

Na primjer:

$$\frac{1}{\sqrt{15}}\left(|00\rangle + 2|01\rangle - |10\rangle - 3|11\rangle\right) \longmapsto \frac{1}{\sqrt{15}}\left(|00\rangle + 2|01\rangle - |11\rangle - 3|10\rangle\right)$$

Mjerenje u sustavu od više qubita

Ako mjerimo prva dva qubita sustava

$$\frac{1}{2}\left(|000\rangle - |001\rangle + |110\rangle + |111\rangle\right)$$

$$\| $$

$$|00\rangle\left(\frac{1}{2}|0\rangle - \frac{1}{2}|1\rangle\right) + |11\rangle\left(\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle\right)$$

izmjerit ćemo $|00\rangle$ s vjerojatnošću $\left(\frac{1}{2}\right)^2 + \left(-\frac{1}{2}\right)^2 = \frac{1}{2}$

$|11\rangle$ -||- $\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$

normalizacija ↓

Ako izmjerimo $|00\rangle$, sustav prelazi u stanje $|00\rangle\left(\frac{1}{2}|0\rangle - \frac{1}{2}|1\rangle\right)\cdot\sqrt{2}$

Kvantna teleportacija

Alice (Zemlja) — Bob (Mars)

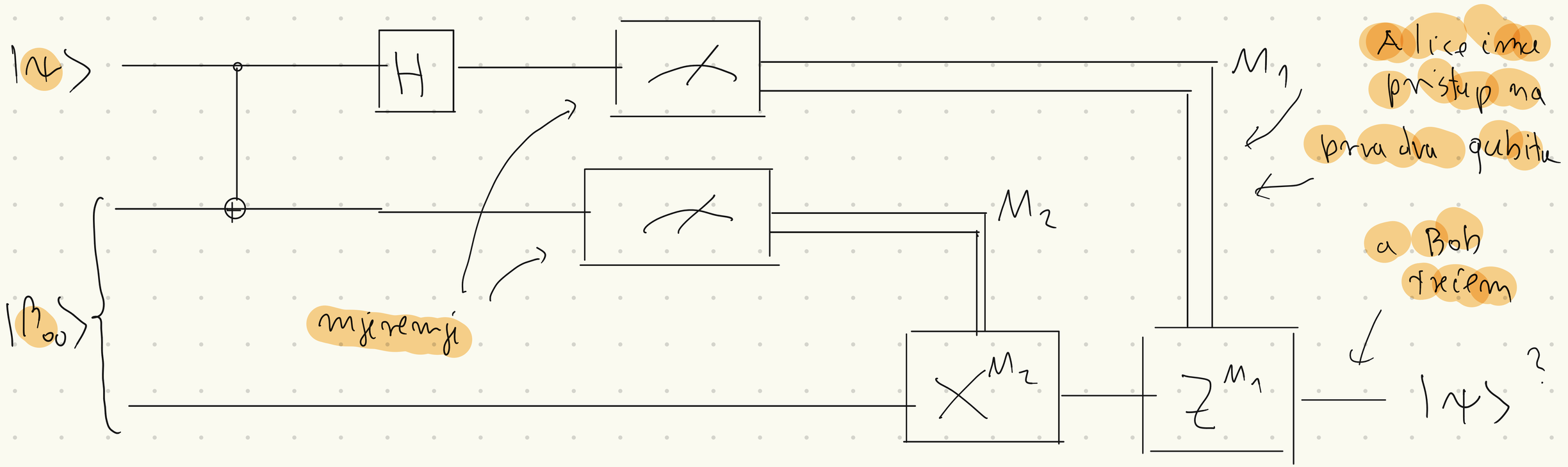
$|\psi\rangle = a|0\rangle + b|1\rangle$ ⇝ ? $|\psi\rangle$

Alice želi teleportirati Bobu qubit $|\psi\rangle$.

Alice i Bob dijele dva qubita u stanju

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

Alice ima pristup prvom, a Bob drugom qubitu.

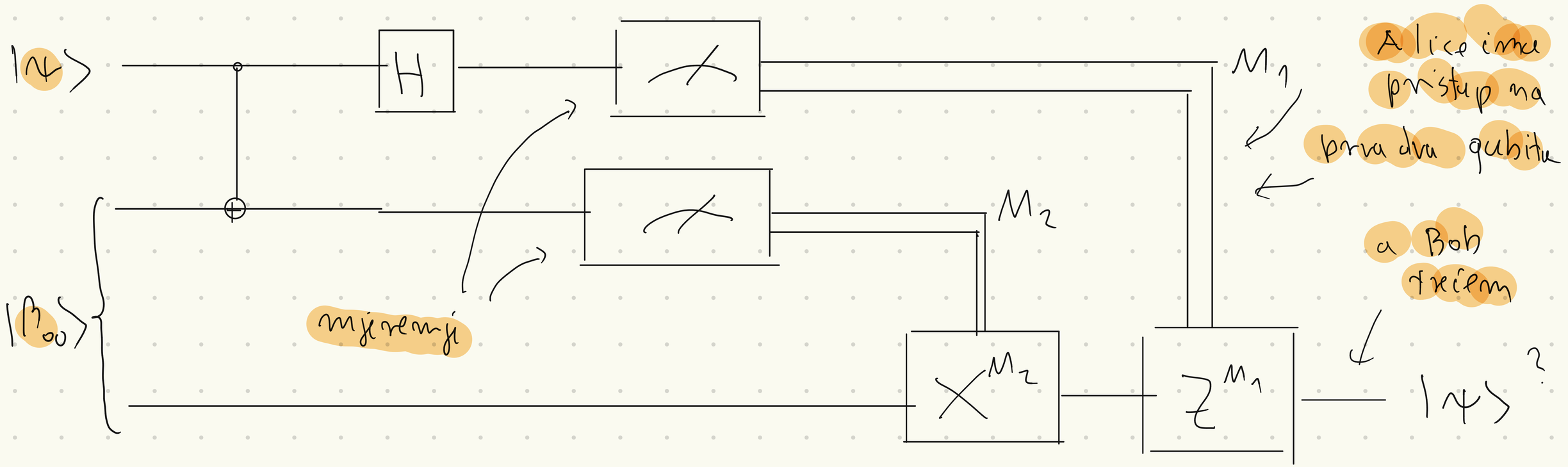


Početno stanje je $|\psi\rangle|\beta_{00}\rangle = (a|0\rangle + b|1\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) =$

$$= \frac{1}{\sqrt{2}}\left(a|0\rangle(|00\rangle + |11\rangle) + b|1\rangle(|00\rangle + |11\rangle)\right)$$

1. korak: Alice primjenjuje CNOT vrata na svoja dva qubita i dobiva stanje

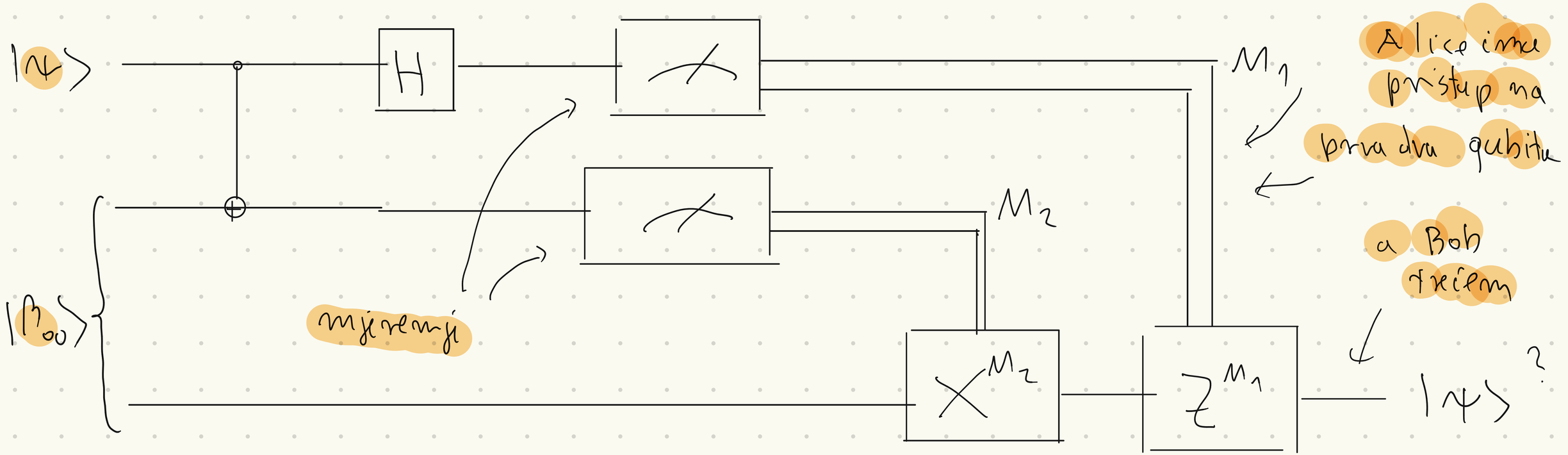
$$\frac{1}{\sqrt{2}}\left(a|0\rangle(|00\rangle + |11\rangle) + b|1\rangle(|10\rangle + |01\rangle)\right)$$



2. korak: Alice primjenjuje Hadamardova vrata na prvi qubit i dobiva

$$\frac{1}{2}\Big[\,|00\rangle(a|0\rangle+b|1\rangle)+|01\rangle(a|1\rangle+b|0\rangle)$$

$$+|10\rangle(a|0\rangle-b|1\rangle)+|11\rangle(a|1\rangle-b|0\rangle)\,\Big]$$



3. korak: Alice mjeri svoja dva qubita i javlja rezultat mjerenja (M_1, M_2) Bobu

$|M_1 M_2\rangle$

Stanja Bobovog qubita ovisno o ishodu mjerenja (M_1, M_2)

$|00\rangle \left(a|0\rangle + b|1\rangle \right)$; $|10\rangle \left(a|0\rangle - b|1\rangle \right)$

$|01\rangle \left(a|1\rangle + b|0\rangle \right)$, $|11\rangle \left(a|1\rangle - b|0\rangle \right)$

4. korak: Ovisno o ishodu mjerenja (M_1, M_2) Bob djeluje na svoj qubit operatorima X i Z kako bi dobio stanje $|\psi\rangle = a|0\rangle + b|1\rangle$

Npr. Ako Alice javi Bobu $(0, 1)$ to znači da se sustav nalazi u stanju $|01\rangle(a|1\rangle + b|0\rangle)$ pa Bob primjenom vrata X na svoj qubit dobiva stanje $|\psi\rangle$

$$X(a|1\rangle + b|0\rangle) = a|0\rangle + b|1\rangle = |\psi\rangle$$

Qubit je uspješno teleportiran.

Deutsch - Jozsa algoritam:

Neka je dana fja. $f: \{0,1\}^n \to \{0,1\}$ za koju znamo da je **konstanta** ili **balansirana** (tj. $\#f^{-1}(0) = \#f^{-1}(1) = 2^{n-1}$). Problem je koristeći što manji poziva fji. f odrediti što je od toga drugi slučaj. Klasično, u najgorem slučaju, nam je potrebno $2^{n-1}+1$ poziv fji. f.

Deutsch - Jozsa algoritam rješava problem s **jednim** pozivom fji. f!

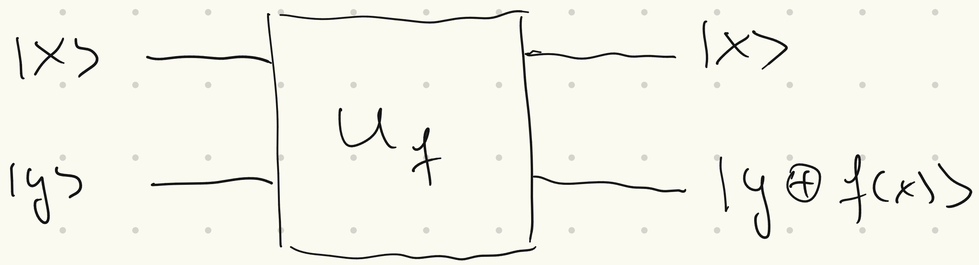
Radi jednostavnosti, pretp. da je $n=1$. (Za vježbu pogledajte algoritam za proizvoljan n.)

unitarni operator

Pretpostavimo da su nam dana kvantna vrata U_f (potprogram) koja proizvoljan element baze $|x\rangle|y\rangle$ preslikavaju u $|x\rangle|y \oplus f(x)\rangle$

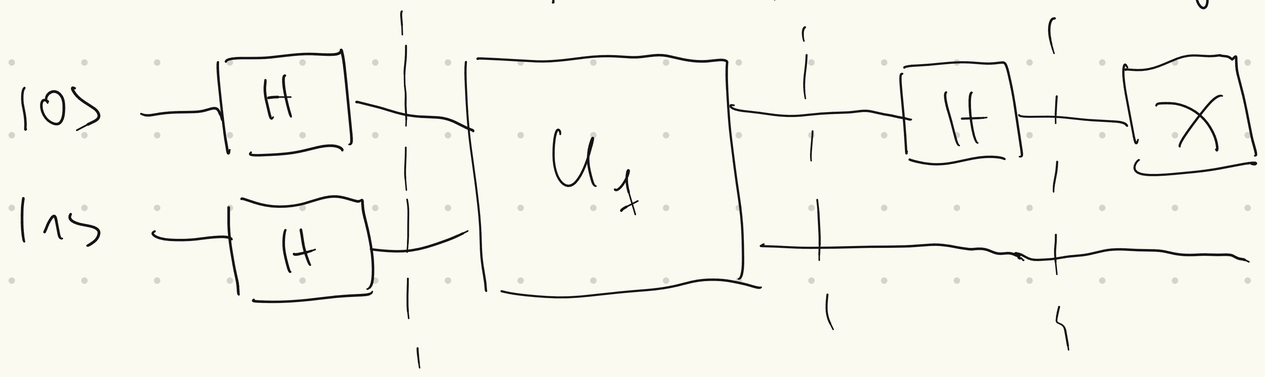
invertibilno preslikavanje

$\oplus$ = XOR ili zbrajanji modulo 2



kvantna proročica

dva qubita] Izračunat ćemo $f(0) \oplus f(1)$ izvršavanjem sljedećeg programa.



← mijenja prvog qubita

Lema: Za $x \in \{0,1\}^n$ vrijedi

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

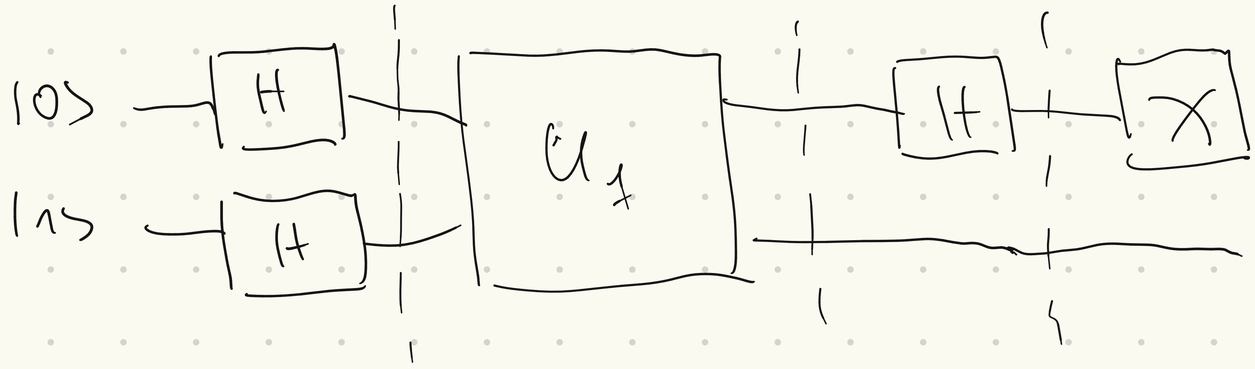
Dokaz: Računamo

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

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

iz čega tvrdnja slijedi analizom slučajeva. ∎

Računamo stanje sustava nakon svake barijere.



- $|\psi_0\rangle = |01\rangle$ početno stanje
- nakon primjene Hadamardovih operatora

$$|\psi_1\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

- primjenom U_f vrata na $|\psi_1\rangle$ dobivamo

$$|\psi_2\rangle = U_f|\psi_1\rangle = U_f\left(|0\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) + U_f\left(|1\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

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

$$= \begin{cases} \pm \dfrac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \dfrac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{ako } f(0)=f(1) \\ \pm \dfrac{|0\rangle-|1\rangle}{\sqrt{2}} \otimes \dfrac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{ako } f(0)\neq f(1) \end{cases}$$

Primjenom Hadamardovog operatora na prvi qubit dobivamo (jer je $H^{-1} = H$)

$$|\psi_3\rangle = \begin{cases} \pm |0\rangle \otimes \dfrac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{ako je } f(0) = f(1) \\ \pm |1\rangle \otimes \dfrac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{ako je } f(0) \neq f(1) \end{cases}$$

Mjerenjem prvog qubita dobit ćemo $|0\rangle$ ako je $f(0) = f(1)$ (tj. ako je f konstanta), odnosno $|1\rangle$ ako je $f(0) \neq f(1)$ (tj. ako je f balansirana).

Jednim pozivom proročice U_f utvrdit ćemo je li fja. f balansirana ili konstanta!

D.Z. Isprogramirajte kvantni algoritam po izboru (u qiskit okruženju) i pokrenite ga na kvantnom računalu u oblaku. Prezentirajte svoje rezultate.

qiskit.org/learn/

M. Karalich: Kvantno računanje (sveučilišni udžbenik)