

Kvantno računanje

Uvod: • Listopad 2019, kvantna prenosc'

Googlovo računalo Sycamore (54 qubita)

200 sec v.s. 10 000 godina
(2.5 dana?)

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

• 1994 Peter Shor

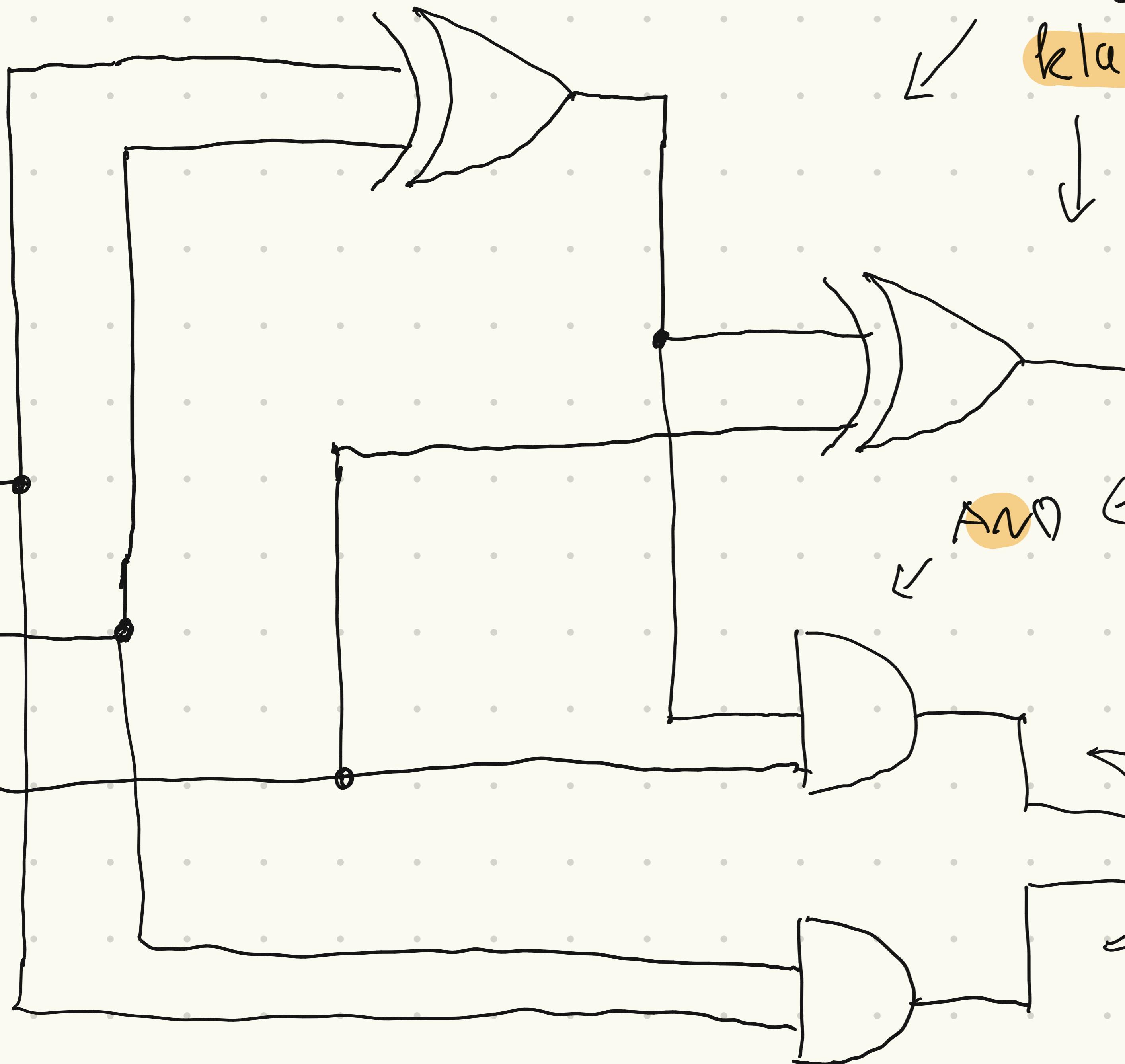
- efikasni algoritam za faktorizaciju
- problem diskretnog logaritma

Sigurnost moderne kriptografije je
bazirana na ova dva problema

- kvantna računala danas: 100 ak qubita, nema zanimljivih primjena
- za faktorizaciju i kriptografiju: 20 milijuna qubita
→ brz razvoj, puni dva tjedna 2 milijarde
- jedna od prvih primjena će biti u simulacijama kemijskih reakcija
- IBM Q (kvantni računalni u oblaku)
i vi možete isprobati (qiskit)
- codeconnects.org kolegij za srednjoškolce

Bit
v.s.
qubit

XOR



Logičké shlopy
klasicky rachunek

$$\text{suma} = A + B + C \bmod 2$$

AND



OR



Logicka vrata

"jedem delji"

zbrajalo

umos

sklop

=

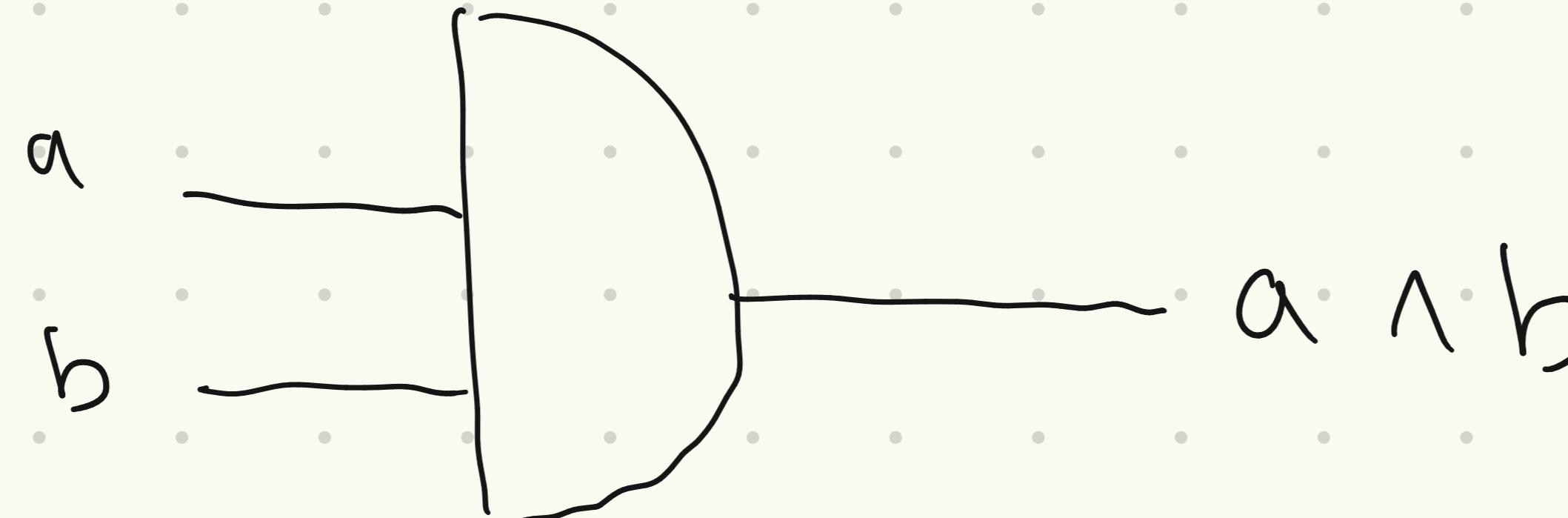
program

izlaz

bit

dva stanje 0 ili 1

Logička vrata



qubit

zbunjujuće, stanje qubita je superpoziciju

stanja $|0\rangle$ i $|1\rangle$

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

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

↗
 \rightarrow
vektor

$$|a|^2 + |b|^2 = 1$$

↑

kompleksni
brojni

no kad želimo očitati stanje qubita (mjeriti)
qubit će se malaziti 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 (izmjeren) qubit koji se načeri

u stanju $|a0\rangle + |b1\rangle$, vjerojatnost da ćemo dobiti

$|10\rangle$ je $|a|^2$ (dok je vjerojatnost za $|11\rangle$ jednaka

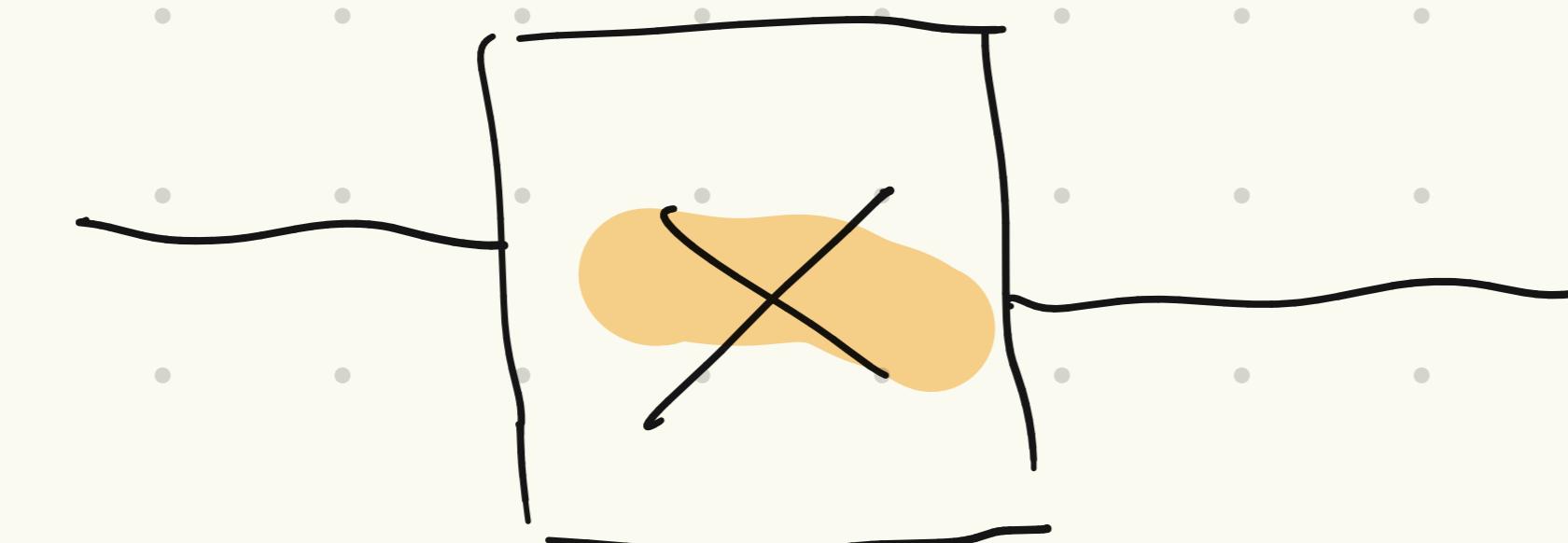
$$1 - |a|^2 = |b|^2$$

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

Kvantna vrata

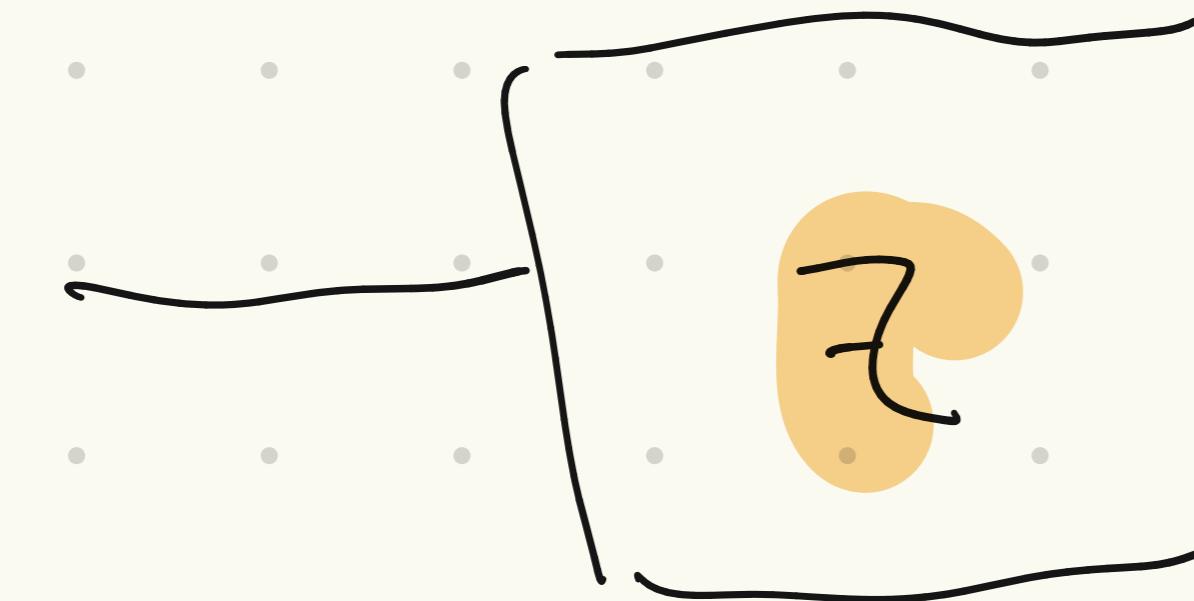
(koja djeluju na jednom qubit)

$|a\rangle + |b\rangle$



$|b\rangle + |a\rangle$

$|a\rangle + |b\rangle$



$|a\rangle - |b\rangle$

$|a\rangle + |b\rangle$



↗ Hadamardova vrata

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

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

Što ako imamo više od jednog qubita?

3 bita mogu biti u jednom
od 8 stanja

sustav od 3 qubita se opisuje
superpozicijom

000
001
010
011
100
101
110
111

$$|\alpha_0|000\rangle + |\alpha_1|001\rangle + |\alpha_2|010\rangle + \dots + |\alpha_7|111\rangle$$

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

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 sistem od ta dva qubita opisuјемо produktom

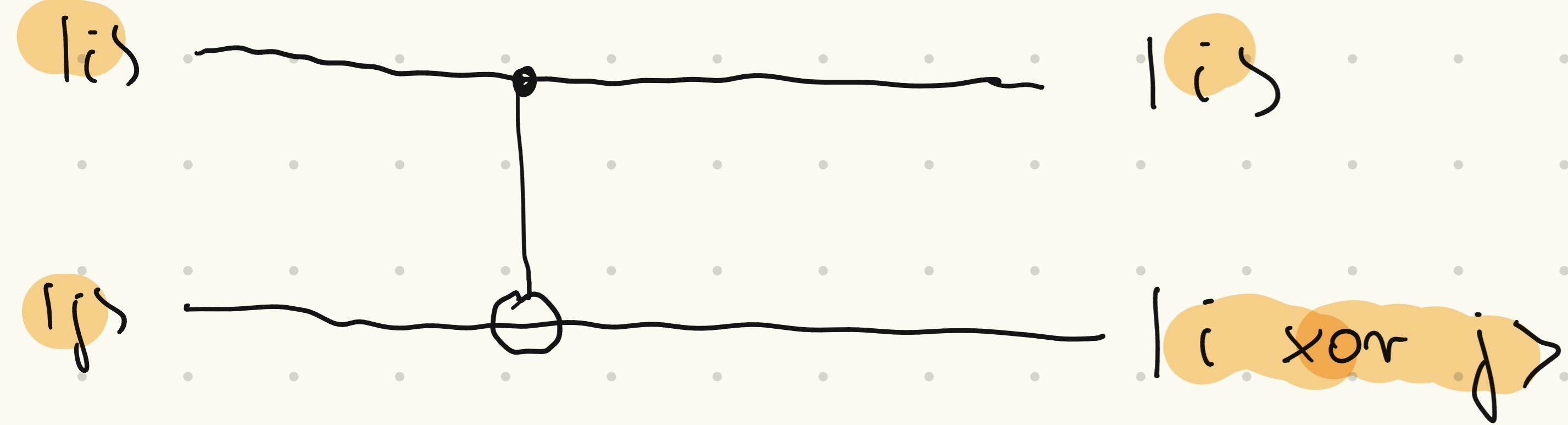
množimo
svaki sa
svakim s time
 $|a|0\rangle|1\rangle + |1\rangle|0\rangle$
" " "
 $|0\rangle$ $|1\rangle$

$$(|a|0\rangle + |b|1\rangle)(|c|0\rangle + |d|1\rangle) = a|100\rangle + a|101\rangle + b|110\rangle + b|111\rangle$$

$$(Uočite \quad |a|^2 + |b|^2 + |c|^2 + |d|^2 = 1)$$

(CNOT operator

(djeluje na dva qubita)



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

Na primjer:

$$\frac{1}{\sqrt{15}} (|00\rangle + 2|01\rangle - |10\rangle - 3|11\rangle) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{15}} (|00\rangle + 2|01\rangle - |11\rangle - 3|10\rangle)$$

Mjerenje u sustavu od više qubitova

Ako mijenjimo prva dva qubita sustava

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

||

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

izmjenit 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 izmjenimmo $|00\rangle$, sustav prelazi u stanju

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

Kvantna teleportacija

Alice (Zemlja)

$$|+\rangle = a|0\rangle + b|1\rangle$$

Bob (Mars)

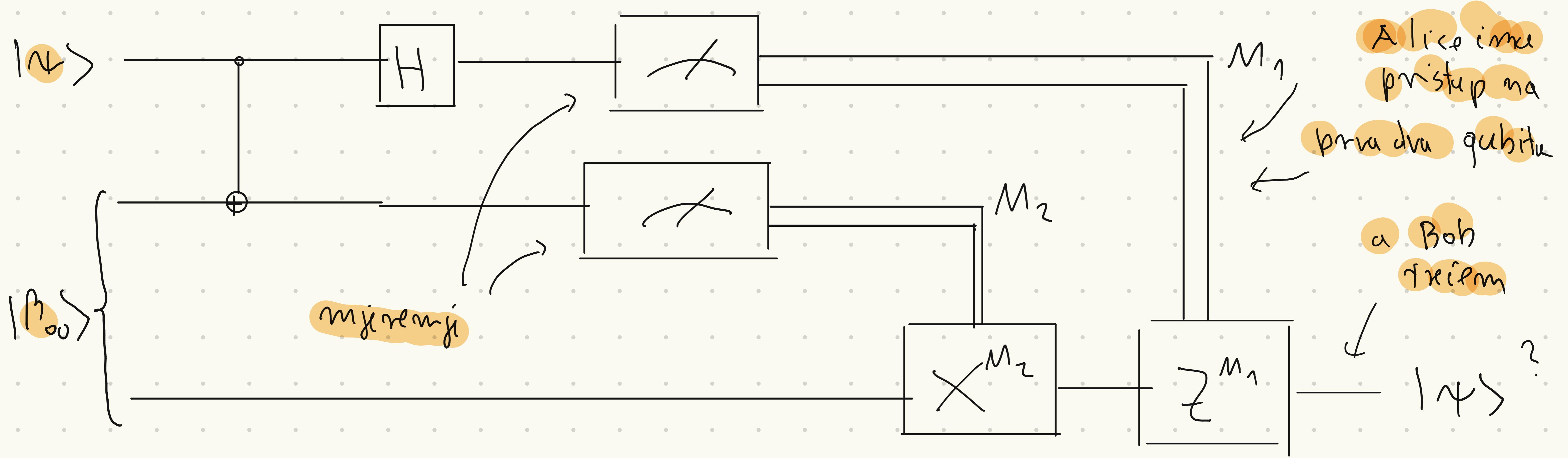
$$? |+\rangle$$

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

Alice i Bob dijle dva qubita u stanju

Alice ima pristup prvom, a Bob drugom qubitu.

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

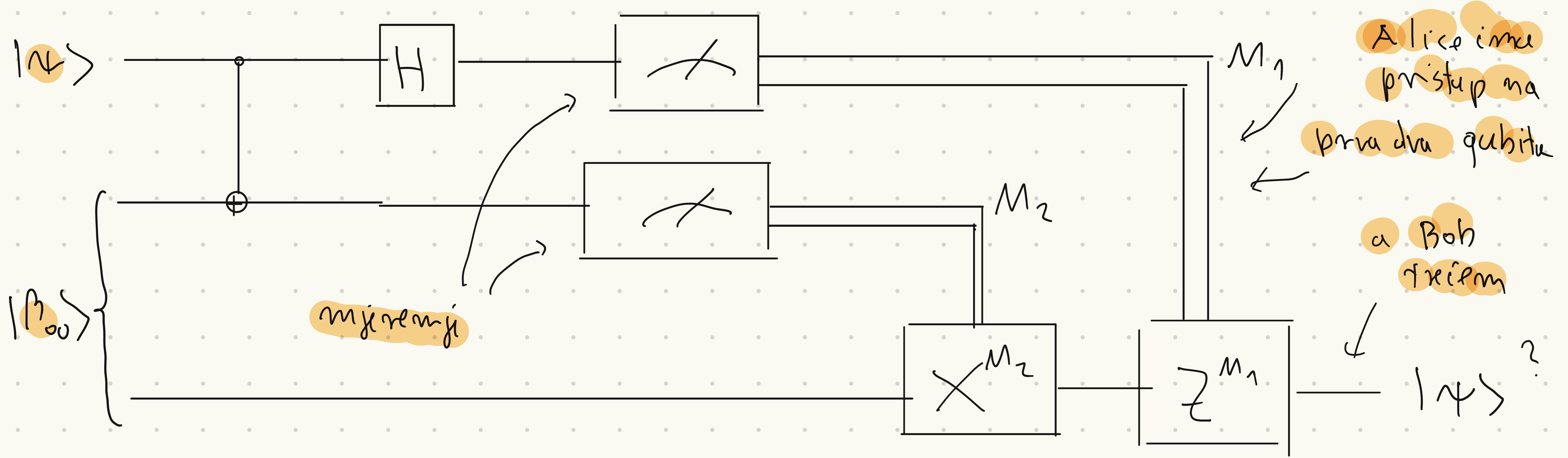


$$\text{Početna stanja su: } |11\rangle |00\rangle = (a|00\rangle + b|11\rangle) \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) =$$

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

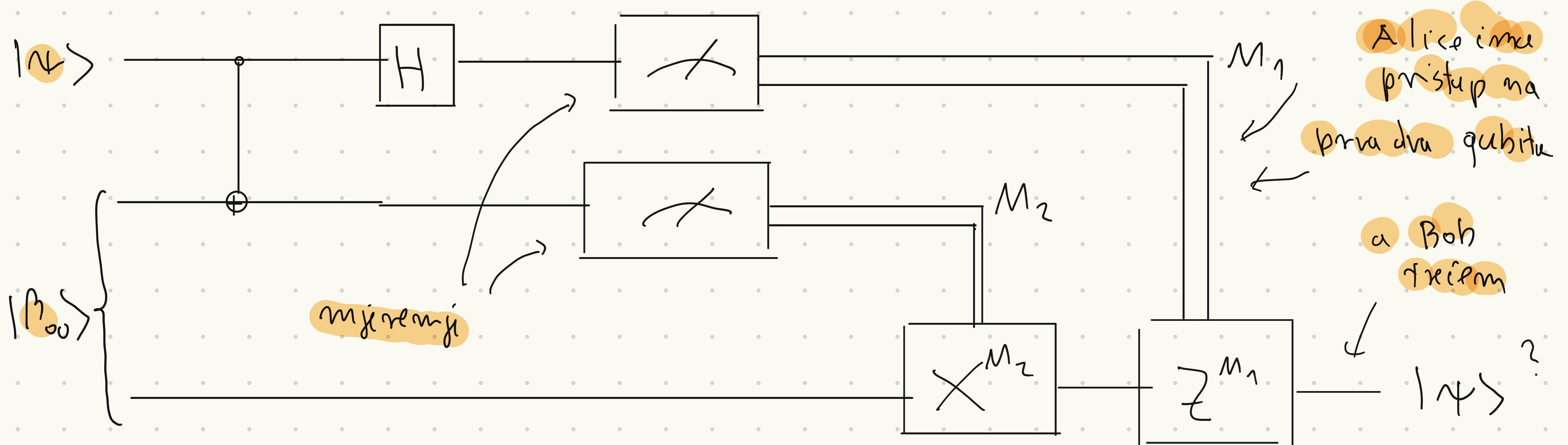
1. korak: Alice primjenjuje $CNOT$ vrata na svoja dva qubita i dobiva stanje

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



2. krok: Alice primířujeji Hadamarovu vrata na prvi qubit i dobiva

$$\frac{1}{2} \left[|00\rangle (|a0\rangle + |b1\rangle) + |01\rangle (|a1\rangle + |b0\rangle) + |10\rangle (|a0\rangle - |b1\rangle) + |11\rangle (|a1\rangle - |b0\rangle) \right]$$



3. korak: Alice mijenja svoja dva qubita i javlja rezultat mijenjanja (M_1, M_2)

$$\begin{aligned}
 &|M_1 M_2\rangle \\
 &: \\
 &|00\rangle (a|0\rangle + b|1\rangle) \xrightarrow{\text{swap}} |10\rangle (a|0\rangle - b|1\rangle) \\
 &|01\rangle (a|1\rangle + b|0\rangle) \xrightarrow{\text{swap}} |11\rangle (a|1\rangle - b|0\rangle)
 \end{aligned}$$

Stanje Boboveg qubita ovisno o ishodu mijenjanja (M_1, M_2)

Bobu

4. korak: Ovisno o ishodu mjerjenja (M_1, M_2) Bob djeluje na svoj qubit operatorma X ; Z kada bi dobio stampi $|N\rangle = |0\rangle + |1\rangle$

Npr. Ako Alice javi Bobu $(0, 1)$ to znači da se sustav

nalazi u stanju $|01\rangle (|0\rangle + |1\rangle)$ pa Bob primjenom vrata X na svoj qubit dobiva stampu $|N\rangle$

$$X(|0\rangle + |1\rangle) = |0\rangle - |1\rangle = |N\rangle$$

I qubit je uspješno teleportiran.