5. Kvantno računanje I

Cilj: Sistemi več kubitov in operacije nanje (kvantna vrata)
Preprosti kvantni protokoli npr. supergosto kodiranje in kvantna teleportacija.
Preprovedi kopiranja.

5.1) Primerjava s klasičnim računalništvom

Turingov stroj (1936): ∞ trak s simboli in tabela pravil.
Abstraktni predstavitev računskega stroja.

Univerzalni Turingov stroj uvede pojem algoritma (= mehanični postopek) ki lahko simulira katerikoli drug postopek.

Church-Turingova teza: Funkcija je algoritmično izračunljiva če in samo če je izračunljiva s Turingovim strojem.

Računanje kubitov obravnavamo abstraktno matematično, a v ozadju je vedno neki fizikalni sistem, ki računa izvaja.
Sodobni računalniki: digitalni, klasično tranzistorsko logiko (Bardeen, Brattain, Shockley '47 => Nobelova '56), implementacija z logičnimi vrati + pomnilniški element + Vhod/izhod.

Informacija je predstavljena s fizikalnim sistemom.

Fizikalni aspekt: - dober opis s klasično mehaniko
- Moorov zakon (1965)
- Miniaturizacija se bliža fundamentalni meji ~kvantni pojavi
- Nezaželeni efekti kvantih pojavov na delovanje (tuneliranje → izgube, fluktuacije med 0 in 1, disipacija toplote)

Kvantno računalništvo: veda o uporabi kvantnih sistemov za obdelavo podatkov. Nov element je „skrita informacija" (zaradi superpozicije) v kvantnih sistemih.

Univerzalni kvantni računalnik (kvantni Turingov stroj) (Deutsch '85)

Vsak kvantni algoritem je opisljiv s kvantnim Turingovim strojem.

Model kvantnih vezij: kvantna vrata po analogiji z linearnimi logičnimi stanji.

Kasneje najdeni algoritmi (Schor '94, Grover '95) odkrijejo rešitev problemov v polinomskem času, ki niso učinkovito rešljivi na klasičnih računalnikih.

Kvantni simulator (Feynman '82): zgradimo sistem B, ki se obnaša enako kot sistem A, a imamo nad njim odličen nadzor.

Odprta vprašanja:

- So in zakaj so kvantni računalniki bolj zmogljivi?
- Katere druzine problemov lahko bolj učinkovito računamo na kvantnih računalnikih?
- Kako velika je množica algoritmov v primerjavi s problemi, ki so učinkovito rešljivi na klasičnih računalnikih?

Glej: quantum algorithm zoo.org (~100 algoritmov)

5.2 Sistem več kubitov

Klasični večdelčni sistemi

$\{\vec{r}_{n_1}, \dots \vec{r}_{n_n}, \vec{p}_{n_1}, \dots, \vec{p}_{n_n}\}$

Kvantni večdelčni sistemi

$H_1 \otimes H_2 \otimes H_3 \otimes \dots$

Hilbertov prostor za sistem več kubitov je podan s tenzorskim produktom posameznih Hilbertovih prostorov.

Primer: 2 kubita. V_1 in V_2 sta vektorska prostora za posamezna kubita. Bazi sta $V_1 = \{|0\rangle, |1\rangle\}$ in $V_2 = \{|0\rangle, |1\rangle\}$.

Baza za $V_1 \otimes V_2 = \{|0\rangle\otimes|0\rangle, |0\rangle\otimes|1\rangle, |1\rangle\otimes|0\rangle, |1\rangle\otimes|1\rangle\}$

Mažne se več linearne kombinacije v 2^2 dim. prostoru. (superpozicija stanj)

Za n kubitov $V = V_1 \otimes V_2 \otimes \dots \otimes V_n$ in dimenzija prostora je 2^n. Eksponentna rast Hilbertovega prostora - glavni razlog zakaj težko simulirati kvantne sisteme s klasičnimi. 50 kubitov $\sim 2^{50} \sim 10^{15}$ kompleksnih amplitud ~ 16 PB podatkov.

Operatorji: $\hat{A}$ operator v V_1 in $\hat{B}$ operator v V_2:

Def: $(A \otimes B)(|v_1\rangle \otimes |v_2\rangle) \equiv A|v_1\rangle \otimes B|v_2\rangle$

↑ Kroneckerjev produkt matričnih reprezentacij.

Primer: Merimo spin v z-smeri prvega in x-smeri drugega kubita.

$(\sigma_z \otimes \sigma_x)(|\uparrow\rangle\otimes|\uparrow\rangle) = \sigma_z|\uparrow\rangle \otimes \sigma_x|\uparrow\rangle = 1|\uparrow\rangle\otimes|\downarrow\rangle =$

$= |\uparrow\rangle\otimes|\downarrow\rangle$

Skalarni produkt: $\left(\sum_i a_i |v_i\rangle\otimes|w_i\rangle, \sum_j b_j |v_j'\rangle\otimes|w_j'\rangle\right) =$

$= \sum_{ij} a_i^* b_j \langle v_i|v_j'\rangle \langle w_i|w_j'\rangle$

Primer: $\langle\uparrow|\otimes\langle\uparrow|(\sigma_z\otimes\sigma_x)|\uparrow\rangle\otimes|\uparrow\rangle = (\langle\uparrow|\otimes\langle\uparrow|)(|\uparrow\rangle\otimes|\downarrow\rangle) = \langle\uparrow|\uparrow\rangle\langle\uparrow|\downarrow\rangle = 0$

5.2.1 Matrični zapis

Ponovimo kronecherjev produkt matrik

$$A \otimes B = \begin{pmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ \vdots & & & \\ A_{m1}B & \cdots & \cdots & A_{mn}B \end{pmatrix}$$

$[m \times n] \quad [p \times q]$

Primer: 2 kubitna stanja $|\uparrow\rangle = \begin{pmatrix}1\\0\end{pmatrix} \quad |\downarrow\rangle = \begin{pmatrix}0\\1\end{pmatrix}$

$$|\uparrow\rangle \otimes |\uparrow\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix} 1\begin{pmatrix}1\\0\end{pmatrix} \\ 0\begin{pmatrix}1\\0\end{pmatrix} \end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

Operatorji $\sigma_z \otimes \sigma_x = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \otimes \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix} 1\begin{pmatrix}0&1\\1&0\end{pmatrix} & 0\begin{pmatrix}0&1\\1&0\end{pmatrix} \\ 0\begin{pmatrix}0&1\\1&0\end{pmatrix} & -1\begin{pmatrix}0&1\\1&0\end{pmatrix} \end{pmatrix} =$

$$= \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

Delovanje operatorja na stanje

$$(\sigma_z \otimes \sigma_x)(|\uparrow\rangle \otimes |\uparrow\rangle) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{bmatrix} \begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} =$$

$$= \begin{bmatrix} 1 & \begin{pmatrix}0\\1\end{pmatrix} \\ 0 & \begin{pmatrix}0\\1\end{pmatrix} \end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = |\uparrow\rangle \otimes |\downarrow\rangle \checkmark$$

Enaka B

Enak rezultat z matričnim množenjem.

Kronecherjev produkt ni komutativen $\sigma_z \otimes \sigma_x \neq \sigma_x \otimes \sigma_z$

Tenzorski produkt sestavljen tako, da vzdržuje načelo superpozicije.

Splošno stanje: $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$

+ nor. normalizacija $\sum_{ij} |\alpha_{ij}|^2 = 1$; 4 kompleksna št = 8 realnih − 2 (normalizacija, globalna faza)

= 6 prostih parametrov | 2 kubita ≠ 2 Blochovi sferi!

5.2.2 Meritev

- opravimo meritev na prvem in z verjetnostjo $p_1 = |\alpha_{00}|^2 + |\alpha_{01}|^2$ izmerimo $|0\rangle$.

- Po meritvi je stanje $|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$

- opravimo meritev na drugem. kubitu. Verjetnost za stanje $|1\rangle$ je $p_2 = \frac{|\alpha_{01}|^2}{|\alpha_{00}|^2 + |\alpha_{01}|^2}$

- Vzamemo eksp. izmerimo, da je sistem v končnem stanju $|01\rangle$ z verjetnostjo $p_3 = |\alpha_{01}|^2$

- Verjetnost za končno stanje $|01\rangle$ je enaka verjetnosti zaporednih meritev

$p_3 = p_1 \cdot p_2$.

$|\alpha_{01}|^2 = \frac{\alpha_{01}^2}{\sqrt{\ldots}} \cdot \ldots$

Lahko merimo v obratnem vrstnem redu, ker

$P(A \cap B) = P(A|B)P(B) = P(B|A)P(A)$

Bayesova formula

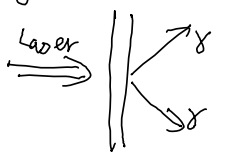
5.3 Bellovo stanje in prepletenost

$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ Pomerimo prvega $|0\rangle$ $\psi' = |00\rangle$ Tudi drugi $|0\rangle$

Pomerimo prvega $|1\rangle$ $\psi' = |11\rangle$ $\Rightarrow$ Tudi drugi $|1\rangle$

Rezultati meritve so korelirani in sprememba je hipna ("spooky action at a distance" - skrivno delovanje na daljavo)

Stanje pripravimo eksperimentalno s parametričnim sipanjem



par koreliranih fotonov z 1/2 energije začetnega fotona

- Korelacije so eksperimentalno dokazane in v Bellovem stanju so močnejše, kot bi jih lahko dobili v katerikoli klasični sistemu (Bellove neenačbe).

- Stanje $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ → Drugi dobi vedno obratno informacijo (sta korelirana).

- Korelacije tudi, če sta podsistema A in B prostorsko ločena, npr. B pošljemo na Luno. Ni možno pošiljati informacij na ta način.

Izpusti nepredavanjih

Podatek: Lahko bi pošiljali informacijo, če bi lahko kopirali kubit (no-cloning theorem)

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

Alice: meri v smeri z $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

prvi kubit $|0\rangle$: $P_0 = |00\rangle\langle 00| + |01\rangle\langle 01| \Rightarrow |\psi'\rangle = |00\rangle$

prvi kubit $|1\rangle$: $P_1 = |10\rangle\langle 10| + |11\rangle\langle 11| \Rightarrow |\psi'\rangle = |11\rangle$

Bob: a) meri σ_z na drugem kubitu vedno $|0\rangle \Rightarrow 000000$ ali $|1\rangle \Rightarrow 111111$ } Rezultati meritve so povsem korelirani.

b) meri v smeri x

$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

prvi kubit v $|+\rangle$: $P_+ = |+\rangle \otimes |0\rangle\langle +| \otimes \langle 0| + |-\rangle \otimes |1\rangle\langle -| \otimes \langle 1| =$

$= \frac{1}{2}(|00\rangle + |10\rangle)(\langle 00| + \langle 10|) + \frac{1}{2}(|01\rangle + |11\rangle)(\langle 01| + \langle 11|)$

$$P_+ |\psi\rangle = \frac{1}{\sqrt{2}} \frac{1}{2} \left(|00\rangle + |10\rangle \right) + \frac{1}{2} \frac{1}{\sqrt{2}} \left(|01\rangle + |11\rangle \right) =$$

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

Recimo, da 1 zneri

00 10 11 10 10

$$P_- |\psi\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle \right) \otimes \left(|0\rangle - |1\rangle \right)$$

10 10 11 1

Rezultati meritev so neodvisni

Iz meritev lahko bob ugotovi katera vrata je Alice uporabljala. Problem: začetnih stanj ne more nam kopirati.

Kvantna prepletenost (entanglement) = večdelčna superpozicija, kjer so meritve korelirane

Ključna lastnost KM sistemov za kvantno komuniciranje, računanje.

Stanje ni prepleteno, če ga znamo zapisati kot tenzorski produkt dveh stanj. Temu rečemo separabilno stanje

Primer: $|\psi\rangle = |00\rangle + |01\rangle + |10\rangle + |11\rangle = \left(|0\rangle + |1\rangle \right) \otimes \left(|0\rangle + |1\rangle \right)$

Rezultat meritev na obeh kubitih povsem nekorelirani.

Bellova stanja so povsem prepletena in tvorijo ortonormirano bazo

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle \right), \quad |\beta_{01}\rangle = \frac{1}{\sqrt{2}} \left(|01\rangle + |10\rangle \right), \quad |\beta_{10}\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle \right)$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}} \left(|01\rangle - |10\rangle \right)$$

Spomli na predavanjih

Entropija prepletenosti ~ koliko "skrite" informacije

Gostotna matrika za zaprt sistem $\rho = |\psi\rangle\langle\psi|$

Entropija $S = -Tr[\rho \ln(\rho)]$ in sebej sistem razlijemo na A in B del. Entropija dela A je $\rho_A = Tr_B(|\psi\rangle\langle\psi|)$ in $\rho_B = Tr_A[|\psi\rangle\langle\psi|]$

Primer: a) Separabilno stanje $|\psi\rangle = |00\rangle$

$$\rho_A = Tr_B[|00\rangle\langle 00|] = \langle 0|_B (|00\rangle + \langle 00|)|0\rangle_B + \langle 1|_B (|00\rangle\langle 00|)|1\rangle_B = |0\rangle_A\langle 0|_A + \emptyset = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$S = -Tr[\rho_A \log(\rho_A)] = -Tr\left[\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \ln\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right] = -Tr\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$$

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

$$\rho_A = Tr_B\left[\frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11| + \frac{1}{2}|00\rangle\langle 11| + \frac{1}{2}|11\rangle\langle 00|\right] =$$

$$= \frac{1}{2}|0\rangle_A\langle 0|_A + \frac{1}{2}|1\rangle_A\langle 1|_A$$

$$S = -Tr[\rho_A \log(\rho_A)] = -Tr\left[\begin{pmatrix} \frac{1}{2} & \emptyset \\ \emptyset & \frac{1}{2} \end{pmatrix} \log\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}\right] = \frac{2}{2}\log 2 = \log 2$$

5.4 Unitarnost

Matrika je unitarna, če $U^\dagger U = U U^\dagger = \mathbb{1}$.

Unitarna matrika ohranja skalarni produkt

$(U|v\rangle, U|w\rangle) = \langle v|U^\dagger U|w\rangle = \langle v|\mathbb{1}|w\rangle = \langle v|w\rangle$.

V kvantni mehaniki to pomeni, da ohranjajo verjetnost (zaprt sistem).

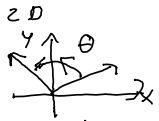
Če $|\langle\psi|\psi\rangle|^2 = 1$, potem $(U\psi\rangle, U|\psi\rangle) = 1$ in $|\psi'\rangle = U|\psi\rangle$ ostane normiran.

Dodatne lastnosti:

a) vse lastne vrednosti imajo dolžino 1: $|\lambda_i| = 1$
in jih lahko zapišemo kot $\lambda_i = e^{i\theta_i}$, $\theta_i \in \mathbb{R}$.

b) $|\det(U)| = 1$

c) V realnih prostorih so to ortogonalni operatorji. Npr. rotacija v 2D



$$R(\theta) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \quad \det(R) = 1$$

Postulat kvantne mehanike: časovno odvisnost kvantnega stanja opišemo z unitarnim operatorjem (za zaprt sistem)

$$|\psi(t = t_2)\rangle = U(t_2, t_1)\,|\psi(t = t_1)\rangle$$

Omejitev na $U(t_2, t_1)$ je ohranitev normalizacije.
Propagacija predstavlja "zasuk" v kompleksnem Hilbertovem prostoru.

Reverzibilnost: $|\psi'\rangle = U|\psi\rangle$ in če pomnožimo z $U^\dagger$: $|\psi'\rangle = U^\dagger U|\psi\rangle = |\psi\rangle$

$U(U^\dagger)$ propagacija naprej (nazaj) v času. KM je reverzibilna.

5.5 Kvantna vezja implementirajo unitarne transformacije

$|\psi'\rangle = U|\psi\rangle$

→ Simbolična reprezentacija algoritmov

Lastnosti: - enojna žička je kvantno stanje in dvojna klasično
- čas teče iz leve proti desni
- enolitne operacije so kvadratki s simbolom

- meritev je označena z 

→ Nereverzibilnost klasičnih vrat:

Primer: AND

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

Informacija se izgubi, ker iz odgovora ne moreš sklepati na input.
To ni možno v kvantnih vezjih.

- kvantna vezja so aciklična = ni zank.
- Ena žička se ne sme razcepiti na več vej. Kopiranje kubitov je prepovedano. Klasično ni problem ("fan-out")

5.5.1 Eno kubitna vrata = unitarna in linearna operacija na 1 kubitu

Primeri: a) Vrata NE (NOT) $|0\rangle \to |1\rangle$, $|1\rangle \to |0\rangle$, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ Razno Paulijeva σ_x

Označimo 

b) Phase-flip Z vrata $|0\rangle \to |0\rangle$, $|1\rangle \to -|1\rangle$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_z$

c) Hadamar vrata (Jacques Hadamard)
Transformacija iz baze lastnih stanj $\sigma_z \{|0\rangle, |1\rangle\}$ v lastna stanja $\sigma_x \{\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\}$

$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $\quad H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ $\quad$ —[H]—

$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

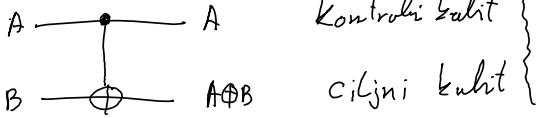
Velja: $H^2 = H^+ H = \mathbb{1}$ $\quad$ in $\quad H = \frac{1}{\sqrt{2}}(X + Z)$

d) Fazna vrata

$S = \begin{pmatrix} 1 & 0 \\ 0 & +i \end{pmatrix}$ $\quad$ —[S]—

e) $\pi/4$ vrata $\quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$ —[T]—

5.5.2 Večkubitna vrata:
Morajo biti reverzibilna ~ problem s klasičnimi AND in NAND

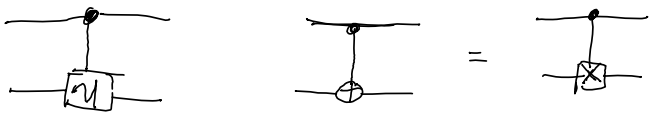
C NOT 

Če kontrolni $|0\rangle$, ni spremembe. Če kontrolni $|1\rangle$, se ciljni obrne $|0\rangle \leftrightarrow |1\rangle$.

$|0\,0\rangle \to |0\,0\rangle$
$|0\,1\rangle \to |0\,1\rangle$
$|1\,0\rangle \to |1\,1\rangle$
$|1\,1\rangle \to |1\,0\rangle$

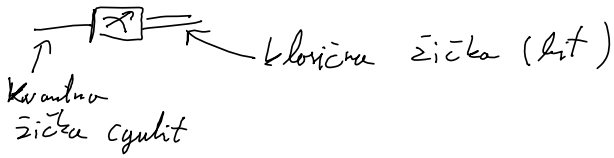
$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

Podobno velja XOR $\quad |A\ B\rangle \to |A\ A\oplus B\rangle$; če $A \oplus B$ seštevanje modulo 2.
Splošna oznaka za kontrolna vrata za operacijo U

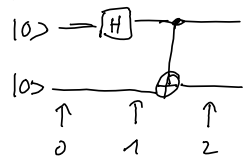


Trditev: poljubna večkubitna vrata lahko sestavimo iz CNOT in enokubitnih vrat. To je kvantni ekvivalent NAND vrat.

Standardni set: CNOT, H, S, T ovegoča odličen približek za poljubna unitarna vrata.

Merilec: 

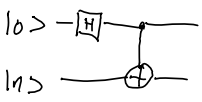
Primer:



0: $|00\rangle$

1: $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle+|10\rangle)$

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



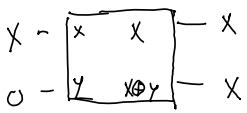
0: $|01\rangle$

1: $\frac{1}{\sqrt{2}}(|01\rangle+|11\rangle)$

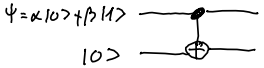
2: $\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle) = \beta_{01}$

E.6 Kvantno kopiranje ("No-cloning" theorem)

klasično



kvantno



Vendar kopija ni lika.

$|\psi\rangle\otimes|\psi\rangle = \alpha^2|00\rangle+\alpha\beta|01\rangle+\alpha\beta|10\rangle+\beta^2|11\rangle$

Torej produkt vezja ni kopija, razen če $\alpha\cdot\beta=0 \Rightarrow$

$$\Rightarrow \begin{cases} \alpha=0, \beta=1 \\ \alpha=1, \beta=0 \end{cases}$$

Klonirano lahko le ortogonalna stanja $|0\rangle$ in $|1\rangle$, ne pa poljubne superpozicije. Vprašanje separabilnosti.

Izpeti

"No-cloning" teorem (Wootters, Zurek '82)

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ $\quad |\psi\rangle \otimes |\psi\rangle = (\alpha|0\rangle+\beta|1\rangle)\otimes(\alpha|0\rangle+\beta|1\rangle)$

Ali obstaja unitarna transformacija U, da $U\,|\psi\rangle\otimes|0\rangle = |\psi\rangle\otimes|\psi\rangle$?

Za poljubni stanji $|\phi\rangle$ in $|\psi\rangle$: $\langle\phi|\psi\rangle = (\langle\phi|\otimes\langle 0|)(|\psi\rangle\otimes|0\rangle) =$

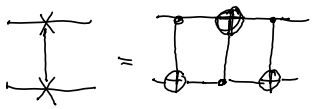
$= (\langle\phi|\otimes\langle 0|)\,U^\dagger U\,(|\psi\rangle\otimes|0\rangle) = (\langle\phi|\otimes\langle\phi|)(|\psi\rangle\otimes|\psi\rangle) = \langle\phi|\psi\rangle^2.$

$$\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2 \Rightarrow \begin{cases} \langle\phi|\psi\rangle = 0; & \text{ortogonalni } \phi\perp\psi \\ |\phi\rangle = e^{i\beta}|\psi\rangle; & \text{če } \langle\phi|\psi\rangle = 1 \end{cases}$$

To nevelja za dve poljubni stanji.

Ne obstaja U, ki bi klonal kvantno poljubno stanje.

SWAP vrata so možna $|ab\rangle \to |ba\rangle$



Dokaz: $|a,b\rangle \to |a, a\oplus b\rangle \to |a\oplus a\oplus b,\ a\oplus b\rangle =$

$= |b,\ a\oplus b\rangle = |b,\ a\oplus b\oplus b\rangle = |b,a\rangle;$

kjer smo uporabili $|x\oplus a\oplus a\rangle = |x\rangle$, ker

$2a \equiv 0 \mod(2)$

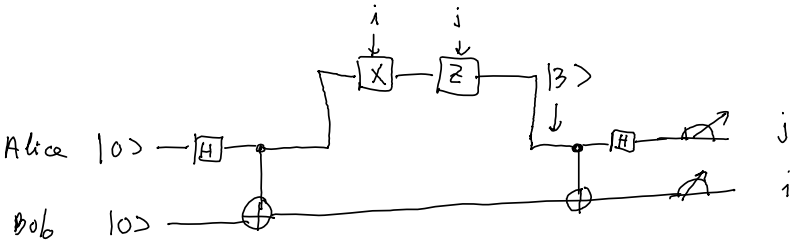
D.N. Poglej direktno za stanja $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

Uvod v giskit (notebook 1)

5.7 Superg gosto kodiranje (Superdense coding) (Bennet + Wiesner 1992)

Protokol, kjer sporočijo superpozicije podvojimo kapaciteto komunikacije. Z enim kubitom oddajemo 2 bita informacije.

(glej notebook 2)



Alice in Bob naredita prepleten par $|00\rangle \to \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \beta_{00}$

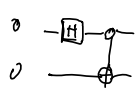
Alice naredi $Z^j X^i$, kjer (j,i) predstavlja 2 klasični biti. Možnosti:

i	j	Operator	Stanje $\|3\rangle$
0	0	I	β_{00}
0	1	Z	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle) = \beta_{10}$
1	0	X	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle) = \beta_{01}$
1	1	$Z \cdot X$	$\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle) = \beta_{11}$

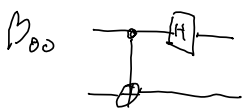
Alice ustvari Bellova stanja, ki so ortogonalna in zato različna z meritvijo.

$ZX = iY = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

Reverzibilnost pove $(U_1 U_2)^\dagger U_1 U_2 = \mathbb{1}$.

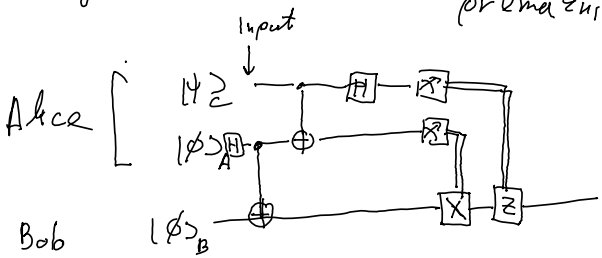
Torej če  β_{00} prepleteta 2 kubita, jih $U_2^\dagger U_1^\dagger$ razpleteta.

Tukaj velja $U_1 = H = H^\dagger$ in $U_2 = CNOT = CNOT^\dagger$. Tako velja

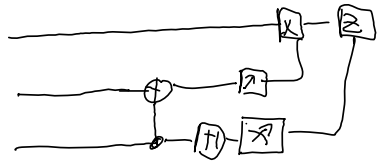


Alice v Bellovo stanje zakodira, 2 bita informacije.

5.8 kvantna teleportacija = stanje kubita prenesemo (glej notebook 3) na drugo mesto, ne da ga pri tem premaknili



$|BAC\rangle$
Beremo od spodaj



$|\psi\rangle_c = \alpha|0\rangle + \beta|1\rangle$

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

$|\phi\rangle_{AB} \otimes |\psi\rangle_c = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \beta|001\rangle + \alpha|110\rangle + \beta|111\rangle)$

$\xrightarrow[\substack{\text{a-tarča}\\ \text{c-control}}]{\text{CNOT}} \frac{1}{\sqrt{2}}(\alpha|000\rangle + \beta|011\rangle + \alpha|110\rangle + \beta|101\rangle) \xrightarrow{H}$

$\xrightarrow{H} \frac{1}{2}(\alpha|000\rangle + \alpha|001\rangle + \beta|010\rangle - \beta|011\rangle + \alpha|110\rangle + \alpha|111\rangle + \beta|100\rangle - \beta|101\rangle)$

Merite:

A C	OPERACIJA	Stanje
0 0	$\mathbb{1}$	$\alpha\|0\rangle + \beta\|1\rangle$
0 1	$\hat{Z}$	$\hat{Z}(\alpha\|0\rangle - \beta\|1\rangle) = \alpha\|0\rangle + \beta\|1\rangle$
1 0	$\hat{X}$	$\hat{X}(\beta\|0\rangle + \alpha\|1\rangle) = \alpha\|0\rangle + \beta\|1\rangle$
1 1	$\hat{Z}\hat{X}$	$\hat{Z}\hat{X}(\alpha\|1\rangle - \beta\|0\rangle) = \hat{Z}(\alpha\|0\rangle - \beta\|1\rangle) = \alpha\|0\rangle + \beta\|1\rangle$

Preneseno

Komentarji: - Alice pošlje dva klasična bita informacije in glede na to Bob popravi svoje stanje
- greza prenos informacije, ne premik fizičnih objektov
(No „Beam me up, Scotty")

- ne nastane kopija, kar je originalno stanje uniči
- ni možno prisluškovanje, ker sta Alice in Bob kvalitet prepletena. Klasični vrednosti ne povesta nič o α in β.