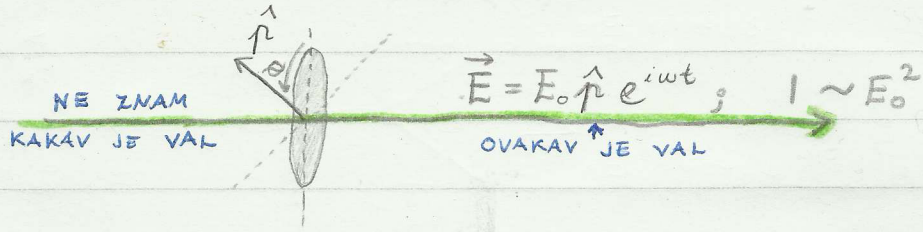
POLARIZACIJA ELEKTROMAGNETSKOG VALA

⇒ prolaskom kroz polarizator, val postaje linearno polariziran

↳ tada znam da nakon polarizatora val titra ovako:

$$\vec{E} = E_0 \hat{p}\, e^{i\omega t}$$

↳ „$e^{i\omega t}$" čitaj jednostavno da val titra frekvencijom „ω"!



$\hat{p}$ → jedinični vektor orijentacije ravnine polarizacije

↳ intenzitet vala nakon polarizatora $\hat{p}$ je proporcionalan kvadratu energije ulaznog vala:

$$I \sim E_0^2$$

⇒ nadalje, sad ako pustimo taj „pomaknuti" val kroz još jedan polarizator (tzv. analizator) dobivamo:

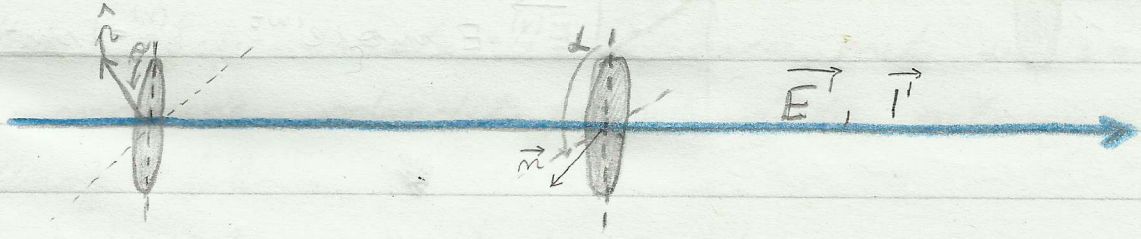
$$\vec{E}' = (\vec{E}\cdot\hat{m})\hat{m} = E_0(\hat{p}\cdot\hat{m})\hat{m}\,e^{i\omega t}$$

$$\vec{E}' = E_0\cos(\theta-\alpha)\,\hat{m}\,e^{i\omega t}$$

↳ ako je $I \sim E_0^2$, onda je novi intenzitet elektromagnetskog vala na izlazu iz analizatora jednak:

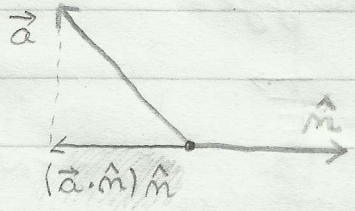
$$\boxed{I' = I\cos^2(\theta-\alpha)}$$

MALUSOV ZAKON



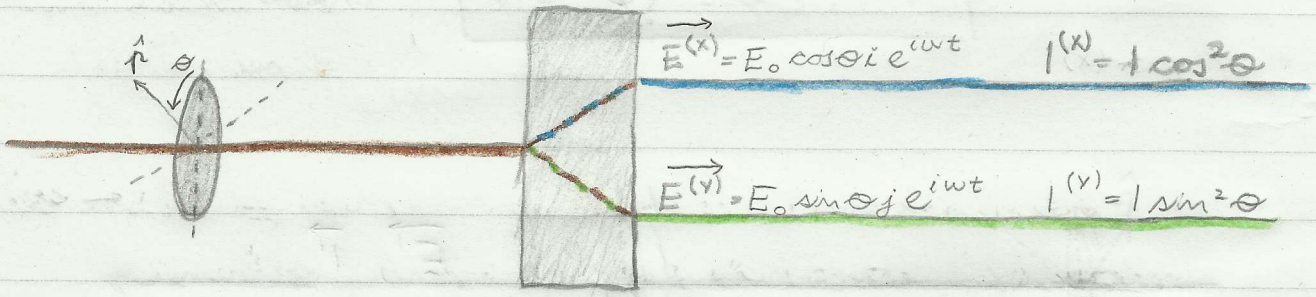
⇒ MATEMATIKA (dodatak):

↳ potrebno za izvod:



RAZDVAJANJE SNOPA POMOĆU KRISTALA

⇒ umjesto analizatora koristimo „dvolomac":
- kristal koji razdvaja svjetlost
- ono što se poklapa s orijentacijom tog kristala ide kroz jedan otvor na izlaz, a sve ostalo ide na drugi izlaz



rastavili smo snop svjetlosti na dva linearno polarizirana snopa s međusobno okomitim smjerovima polarizacije

↳ vrijedi očuvanje energije:

$$\vec{E}^{(x)} + \vec{E}^{(y)} = \vec{E}$$

BITNO!

$$I^{(x)} + I^{(y)} = I$$

POLARIZACIJA FOTONA

⇒ u kvantnoj fizici, svjetlost gledamo kao niz fotona

⇒ danas, eksperimentalno je moguće oslabiti snop svjetlosti i brojiti detektorom svaki foton

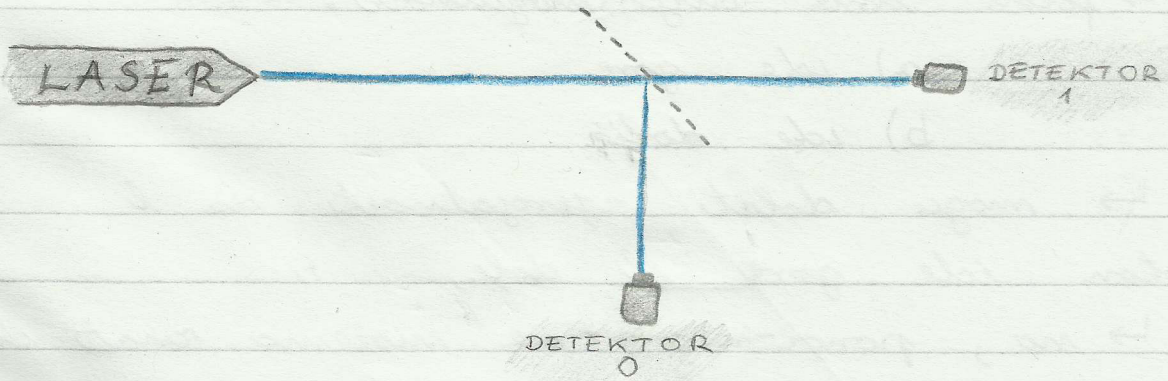
↳ intenzitet svjetlosti razmjeran je broju fotona koji prođu nekom površinom u jedinici vremena:

$$I \sim \frac{dN}{dt}$$

} ta možemo vidjeti veru između klasične i kvantne fizike

⇒ postoje eksperimenti u kojima <u>niti u načelu</u> nije moguće odrediti / predvidjeti gibanje pojedinog fotona

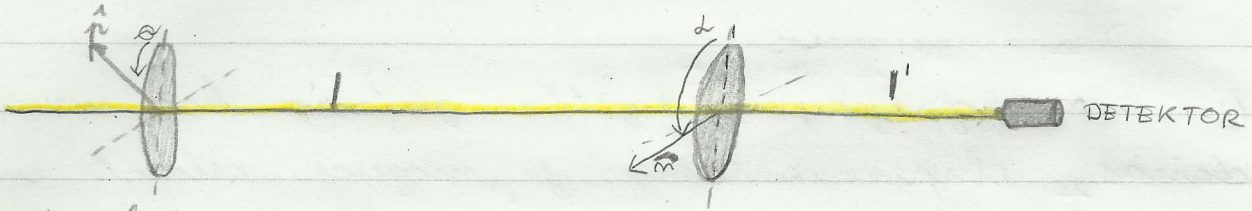
↳ tek u mnoštvu fotona možemo odredit vjerojatnost putanje fotona



⇒ ovime se mogu generirati <u>pravi slučajni brojevi</u>

(naravno, treba kristal sa 50% vjerojatnosti za 0 i 1)

⇒ ako pogledamo opet klasičan polarizator i analizator:



↳ foton ima dvije mogućnosti:

a) ili je pojeden u analizatoru

b) il je došao do detektora

↳ tim spoznajama, mi na osnovu izračuna intenziteta iz klasične (valne) fizike možemo dobiti vjerojatnost prolaska fotona do detektora

BITNO!!

$$p(\Theta \to \perp) = \frac{I'}{I}$$

ovo je vrsta klasičnih (valnih) i kvantnih (čestičnih) spoznaja

$$p(\Theta \to \perp) = \cos^2(\Theta - \perp)$$

⇒ istu stvar možemo napravit na eksperimentu s kristalom s dvije putanje

↳ foton ima dvije mogućnosti:

a) ide gore

b) ide dolje

↳ mogu dobiti vjerojatnosti da l foton ide gore il dole

↳ no, ponovimo - ne možemo znati da l će foton ići gore il dolje

⇒ napravimo sada sljedeći pokus:

- polarizator
- dvolomac
- skupljanje svjetlosti (zrcala il još jedan dvolomac)
- analizator

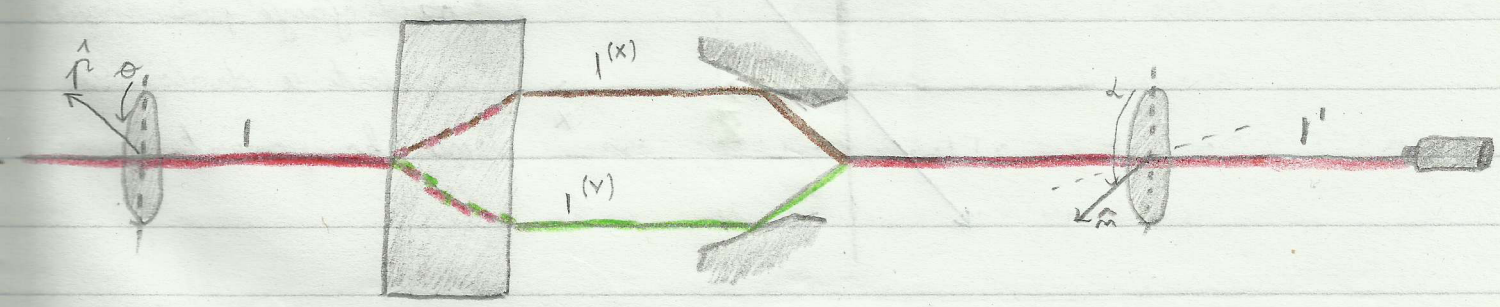
↳ dvolomac ovdje služi kako bi znali kako je određen foton polariziran (za to služi i u prethodnim pokusima)

↳ DVIJE FORMULE NA SLAJDU 8:

- pokazuju da se ne slažu kvantno i klasično objašnjenje
- zbrajanjem vjerojatnost prolaska onih koji idu gore i onih idu dolje ne dobijemo istu vjerojatnost koju opažamo eksperimentom
- gdje je greška?

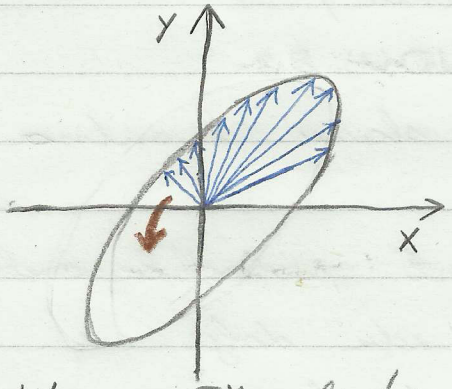
↳ u promatranju (i pretpostavci) koliko fotona ide gore, a koliko fotona ide dolje

↳ jednom kada promatramo fotone na izlazu iz dvolomca, to više nisu ist fotoni koje opažamo na detektoru //



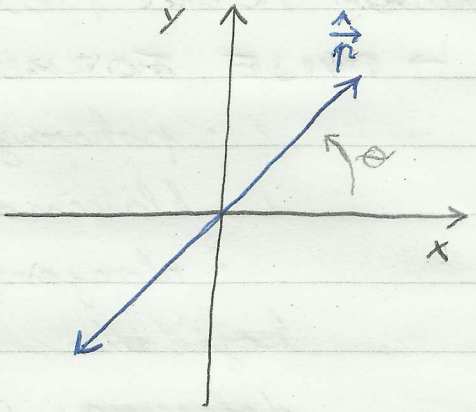
⇒ zbog ovog problema, nećemo pričati o vjerojatnosti nego o **amplitudi vjerojatnosti**

⇒ pokazalo se da je na mikroskopskoj razini priroda nepredvidiva, pa ima smisla pričati o vjerojatnostima, a ne o konkretnim ishodima



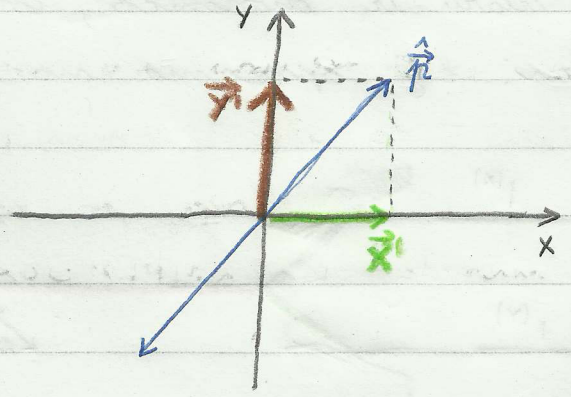
• titranje EM-polja (i fotona) nepolarizirane svjetlosti kruži po elipsi

polarizacija u polarizatoru



• titranje EM-polja (i fotona) polarizirane svjetlosti

razdvajanje polarizirane svjetlosti u dvolomcu



• razdvajanje polarizirane svjetlosti u dvolomcu na komponente

AMPLITUDA VJEROJATNOSTI

⇒ vratimo se na pokus u kojem smo naišli na paradoks:

- paradoks je u tome da mi mislimo da možemo znati koj foton je prošao gore, a koj dolje
- to nit u načelu ne možemo znati

pa slijedeći račun „ne štima":

$$p(\circ \to \downarrow) = p(\circ \to x \to \downarrow) + p(\circ \to y \to \downarrow) = \dots$$

to ne valja!

↳ ne možemo znati kojim putem je foton išao

⇒ da u ovoj pokus umjesto dvolomca stavimo polarizator, račun bi se poklapao sa klasičnom fizikom

⇒ kvantna mehanika traži od nas da vjerojatnost ne računamo na prejednostavan način, pa uvodimo novu fizikalnu veličinu koja je intrinzično kompleksna, a naziva se AMPLITUDA VJEROJATNOSTI

⇒ **AMPLITUDA VJEROJATNOSTI:**

↳ amplituda vjerojatnosti prelaska $\alpha \to \beta \to \gamma$:

$$\boxed{a(\alpha \to \beta \to \gamma) = a(\alpha \to \beta) \cdot a(\beta \to \gamma)}$$

↳ ako ovo primjenimo na eksperiment s dvije putanje, račun se poklapa sa klasičnim viđenjem

⇒ eksperiment s dvije putanje:

- uzmimo za jednostavnost realne amplitude vjerojatnosti prijelaza:

$$a(\theta \to x) = \cos\theta \qquad a(x \to \alpha) = \cos\alpha$$
$$a(\theta \to y) = \sin\theta \qquad a(y \to \alpha) = \sin\alpha$$

(ovo smo s „naštelal" - vidimo da ovo još nisu kompleksni brojevi)

- vjerojatnost prelaska za gornje amplitude vjerojatnosti:

$$a(\theta \to \alpha) = a(\theta \to x)\, a(x \to \alpha) + a(\theta \to y)\, a(y \to \alpha)$$
$$= \cos\theta \cos\alpha + \sin\theta \sin\alpha$$
$$= \cos[\theta - \alpha]$$

↘ modul i kvadrat daje klasičnu vjerojatnost

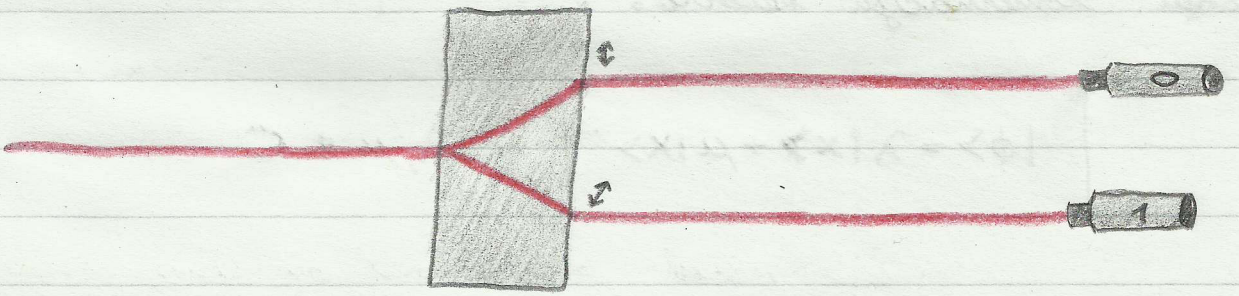
⇒ NAJČEŠĆA INTERPRETACIJA: nema eksperimentalnog odgovora na putanju fotona, pa se smatra da razmišljanje o putanj vod krivom razmišljanju

↳ neke interpretacije kažu: „foton je prošao kroz oba prolara dvolomca"

↳ najbolje što imamo je ovo, i vidimo da račun vrijedi, pa najbolje je uzjeti se da je to tako i naučit računat ☺

⇒ REALIZACIJA KVANTNOG BITA:

- foton može bit u bilo kojem od beskonačno mnogo stanja polarizacije (linearna polarizacija različitih smjerova ili općenita eliptična polarizacija), no mjerenjem je moguće dobit samo dvije različite vrijednosti (nula il jedan)



- polarizator je moguće orjentirat na različite načine što znači da je mjerenje moguće provest na različite načine
- **problem**: foton se može detektirat samo jednom

⇒ KVANTNI BIT (Qubit): kvantnomehanički sustav koj je mjerenjem moguće detektirat u jednom od dva moguća stanja (npr. polarizacija fotona)

BRA-KET (DIRACOVA) NOTACIJA

⇒ notacija za računanje amplitude vjerojatnosti

↳ desna zagrada : KET ⇒ $|X\rangle$

↳ lijeva zagrada : BRA ⇒ $\langle X|$

⇒ stanje polarizacije fotona koj je linearno polariziran u „X" i onog koj je linearno polariziran u „Y" smjeru prikazujemo **ket**-simbolima:

$$|X\rangle \quad , \quad |Y\rangle$$

⇒ bilo koje stanje polarizacije fotona prikazujemo kao linearnu kombinaciju ketova:

$$\boxed{|\phi\rangle = \lambda|X\rangle + \mu|X\rangle} \qquad \lambda, \mu \in \mathbb{C}$$

⇒ u matematičkom smislu, ketovi su vektori dvodimenzionalnog kompleksnog Hilbertovog vektorskog prostora $\mathcal{H}^2$
(vektorski prostor s kompleksnim koeficijentima)

⇒ OPERACIJE:

- zbrajanje vektora
- množenje skalarom
- skalarni produkt
- norma vektora

⇒ skalarni produkt u Hilbertovom prostoru:

- oznaka: $\langle \Psi | \Phi \rangle$
- vrijed: $\langle \Phi | \Phi \rangle \geq 0$ (realni broj)
- vrijed: $\langle \Psi | \Phi \rangle = \langle \Phi | \Psi \rangle^* \in \mathbb{C}$

(kompleksno konjugiran broj ako zamijenimo redoslijed)

⇒ simbol $\langle \Phi |$ se zove **bra** simbol

⇒ simbol $\langle \Phi | \Psi \rangle$ se zove **braket** simbol

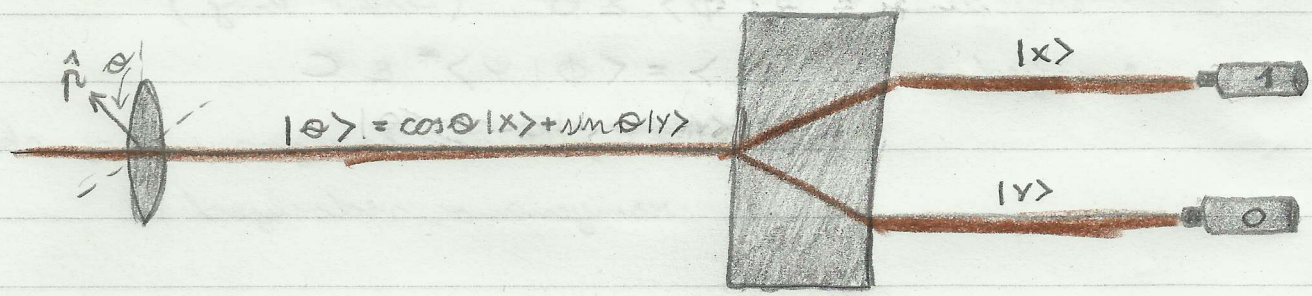
⇒ ako su stanja polarizacije fotona prikazana normiranim vektorima, tada skalarni produkt tih vektora odgovara AMPLITUDI VJEROJATNOSTI da foton u stanju polarizacije $|\Phi\rangle$ bude izmjeren u stanju $|\Psi\rangle$

BITNO!

⇒ spomenimo i normu vektora:

$$\|\Phi\| = \sqrt{\langle \Phi | \Phi \rangle}$$

PR: Mjerenje stanja polarizacije linearno polariziranog fotona!



$$p(\theta \to x) = |a(\theta \to x)|^2 = |\langle x|\theta\rangle|^2 =$$

$$= \left|\langle x|\left(\cos\theta|x\rangle + \sin\theta|y\rangle\right)\right|^2 =$$

$$= \left|\cos\theta \underbrace{\langle x|x\rangle}_{=1} + \sin\theta \underbrace{\langle x|y\rangle}_{=0}\right|^2 =$$

$$= |\cos\theta|^2 = \cos^2\theta$$

↓

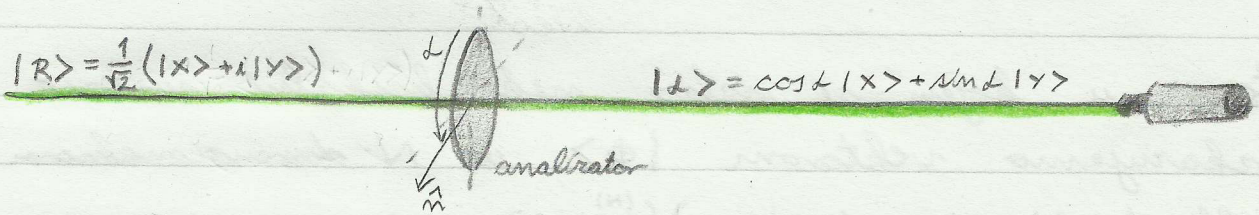
ovo je vjerojatnost koja se slaže sa klasičnim izračunima

$$p(\theta \to y) = |\langle y|\theta\rangle|^2 = \sin^2\theta$$

PRS: Vjerojatnost detekcije cirkularno polariziranog fotona ?

↳ njega označavamo:

$$|R\rangle = \frac{1}{\sqrt{2}}\left(|x\rangle + i|y\rangle\right)$$



$$p(R \to \alpha) = |a(R \to \alpha)|^2 = |\langle \alpha | R\rangle|^2 =$$

$$= \left|\left(\cos\alpha\langle x| + \sin\alpha\langle y|\right)\left(\frac{1}{\sqrt{2}}|x\rangle + i\cdot\frac{1}{\sqrt{2}}|y\rangle\right)\right|^2$$

$$= \left|\frac{\cos\alpha}{\sqrt{2}} + i\frac{\sin\alpha}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

⇓

vjerojatnost detektiranja fotona ne ovisi o orijentaciji polarizatora //

PRINCIPI KVANTNE MEHANIKE

⇒ sada ćemo se upoznat sa osnovnim pojmovima koji nam trebaju za kvantno računanje ▽

⇒ stanje u kojem se nalazi neki fizikalni sustav prikazujemo vektorom $|\Phi\rangle$ u N-dimenzionalnom Hilbertovom prostoru $\mathcal{H}^{(N)}$

↳ vektor $|\Phi\rangle$ nazivamo VEKTOROM STANJA

↳ normiranost podrazumijeva:

$$\langle\Phi|\Phi\rangle = 1$$

⇒ za „n" qbita, treba nam 2^n dimenzionalni Hilbertov prostor, pa je stoga teško simulirat kvantno računalo klasičnim računalom:

- za 3 qbita prostor je 8-dimenzionalan, pa trebamo matrice 8×8 za opis stanja sustava
- vidimo da simulacija kvantnog računala od 20 qbita nije ravnsliva jer su matrice dimenzija $2^{20} \times 2^{20}$

⇒ MJERENJE: (Ψ - provjera)

• izmjeriti sustav u stanju $|\Psi\rangle$ znači da je sustav podvrgnut postupku koji ga dovodi u to stanje te ga u tom stanju (povratno) detektira

⇒ <u>vjerojatnost prelaska sa Φ na Ψ:</u>

• računa se ovako: $\underbrace{\langle\Psi|\Phi\rangle}$ skalarni umnošci u Hilbertovom prostoru

⇒ <u>projekcija stanja $|\Phi\rangle$ na stanje $|\Psi\rangle$:</u>

• računa se ovako: $\underbrace{|\Psi\rangle\langle\Psi|\Phi\rangle}$ analogno skalarnom umnošku

• postoji operator projekcije jer nam projekcija često treba:

$$P_\Psi = |\Psi\rangle\langle\Psi|$$ } projektor na stanje Ψ

⇓

ovo nazivamo PROJEKTOR!

⇒ RELACIJA POTPUNOSTI:

• ako zbrojimo projektore svih vektora bare ortonormiranog prostora $H^{(N)}$, dobivamo jedinični operator:

$$\boxed{\sum_{m=1}^{N} |m\rangle\langle m| = I}$$

⇒ KOMUTATOR OPERATORA:

• operato definiran nad operatorima A i B:

$$[A, B] = AB - BA$$

• ako je komutator jednak nul, ti operatori A i B komutiraju, pa smijemo izmijeniti njihov redoslijed

⇒ KOMPATIBILNE I NEKOMPATIBILNE PROVJERE:

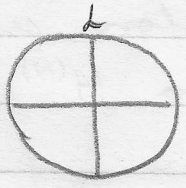
• ako operatori stanja komutiraju, to nam omogućava mjerenje

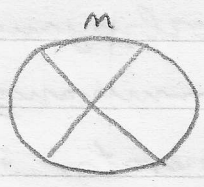
• ako operatori komutiraju, stanja su kompatibilna (okomita), pa je moguće istovremeno provesti provjeru oba stanja

• ako ne komutiraju, nije moguće istovremeno provesti provjeru (kvantna mehanika je takva inherentno)

⇒ <u>maksimalno nekompatibilne provjere:</u>

↳ maksimalno nekompatibilne baze su one koje su pod 45° zakrenute





} N-dimenzionalni Hilbertov prostor

↳ za baze vrijedi: $|\langle L|M\rangle|^2 = \frac{1}{N}$

⇒ kako izmjeriti energiju kvantnog sustava?

↳ jedno mjerenje dobivamo sa nekom vjerojatnošću, drugo s drugom vjerojatnosti, ...

↳ stoga, radimo teorijski prosjek:

$$\underbrace{\sum_n a_n p(\phi \to n)}$$

ovo je srednja očekivana energija koju mjerimo

↳ ovo možemo raspisati:

$$\sum_n a_n p(\phi \to n) = \sum_n a_n |\langle n|\phi\rangle|^2 = \dots$$

$$= \sum_n a_n |n\rangle\langle n| \quad ; \quad a_n \in \mathbb{R}$$

BITNO!!

⇓

ovo je izvod hermitskog operatora

⇒ HERMITSKI OPERATOR:

• služi za mjerenje klasičnih veličina sustava kao što je energija, snaga, ...

$$\boxed{M = \sum_{n=1}^{N} a_n P_n}$$

a_n → svojstvena vrijednost (realan broj)

n → svojstven vektor

$$M = \sum_{n=1}^{N} a_n |n\rangle\langle n|$$

PR: Mujeri se da Hermitski operator stvarno daje svojstvene vrijednosti?

$$M|m\rangle = \left(\sum_n a_n |n\rangle\langle n|\right)|m\rangle$$

$$= \sum_n a_n |n\rangle \underbrace{\langle n|m\rangle}_{=0 \ \forall n \neq m}$$

$$= a_m |m\rangle$$

↓

koeficijent koji opisuje fizikalne veličine vezane uz stanje „m"

⇒ EVOLUCIJA (PROMJENA) STANJA U VREMENU:

- ovo opisuje Schrödingerova jednadžba
- evolucija stanja kvantnog sustava u vremenu $|\Phi[t_1]\rangle \rightarrow |\Phi[t_2]\rangle$ jest <u>linearna transformacija</u> početnog stanja sustava koja tijekom vremena <u>ne mijenja normu vektora stanja</u>
- linearnost daje da gornju relaciju možemo izraziti sa: $|\Phi[t_1]\rangle = U[t_1, t_2]\,|\Phi[t_2]\rangle$, gdje je $U[t_1, t_2]$ operator vremenske evolucije koj ima svojstvo **unitarnosti**

(iz toga slijede mnoga svojstva koja vrdi na slajdovima!)

↳ iz unitarnosti slijedi jednadžba gibanja kvantne mehanike:

$$i\hbar \frac{d}{dt} U[t, t_0] = \hat{H}[t] \cdot U[t, t_0]$$

SCHRÖDINGEROVA JEDNADŽBA

⇓

<u>primjeti</u>: nema druge derivacije (akcelracije) u jednadžbi gibanja kvantne mehanike, al inherentno dolare kompleksni brojevi

($\hat{H}[t]$ je hermitski operator koj opisuje energiju)

↳ *vrsta jednadžbe u Diracovoj notaciji:*

• *pomnoženo sa početnim stanjem* $|\psi[t_0]\rangle$:

$$i\hbar \frac{d}{dt} U[t,t_0] \cdot |\psi[t_0]\rangle = \hat{H}[t]\, U[t,t_0]\, |\psi[t_0]\rangle$$

$$|\psi[t]\rangle$$

• *to je to:*

$$\boxed{i\hbar \frac{d}{dt} |\psi[t]\rangle = \hat{H}[t]\, |t[t]\rangle}$$

⇒ *vid da u oba slučaja treba znat Hamiltonijan sustava (hermitski operator za energiju)*

PR: Neka dvojna okomitim stanjima $|0\rangle$ i $|1\rangle$ glita odgovarajuće energije $\hbar\omega_0$ i $\hbar\omega_1$, pri čemu vrijedi da je $\omega_1 \geq \omega_0$?

↳ treba pronaći hamiltonijan:

$$\hat{H} = \hbar\omega_0 |0\rangle\langle 0| + \hbar\omega_1 |1\rangle\langle 1|$$

↳ drugo, treba napisati stanje sustava (glita):

$$|\Phi[t]\rangle = \mu[t]\,|0\rangle + \lambda[t]\,|1\rangle$$

• početni uvjeti: $\mu[0] = \mu_0$

$\lambda[0] = \lambda_0$

↳ sada možemo u Schrödingerovu jednadžbu:

$$i\hbar\left(\dot{\mu}|0\rangle + \dot{\lambda}|1\rangle\right) = \left(\hbar\omega_0|0\rangle\langle 0| + \hbar\omega_1|1\rangle\langle 1|\right)\cdot \left(\mu|0\rangle + \lambda|1\rangle\right)$$

$$i\hbar\left(\dot{\mu}|0\rangle + \dot{\lambda}|1\rangle\right) = \hbar\left(\mu\omega_0|0\rangle + \lambda\omega_1|1\rangle\right)$$

↳ izjednačimo ono uz $|0\rangle$ i ono uz $|1\rangle$:

$$\left.\begin{aligned} i\dot{\mu} &= \mu\omega_0 \\ i\dot{\lambda} &= \lambda\omega_1 \end{aligned}\right\}$$ rješimo ovaj diferencijalni sustav separacijom varijabli

OKRENI →

↳ rješimo prvu: $i \cdot \frac{d\mu}{dt} = \mu \omega_0$

$$\frac{d\mu}{\mu} = -i\omega_0 \, dt$$

$$\frac{\mu}{\mu_0} = e^{-i\omega_0 t} \Rightarrow \mu[t] = \mu_0 e^{-i\omega_0 t}$$

↳ analogno, rješenje druge je: $\lambda[t] = \lambda_0 e^{-i\omega_1 t}$

↳ uvrstimo natrag u Schrödingerovu jednadžbu i to je to:

$$|\Phi[t]\rangle = \mu_0 e^{-i\omega_0 t}|0\rangle + \lambda_0 e^{-i\omega_1 t}|1\rangle$$

⇒ vid se da se fazni odnos između nule i jedinice tijekom vremena mijenja

⇒ NAPOMENA: na ispitu nećemo trebat ovo rješovati, već je samo za demonstraciju (i osobni užitak)

KVANTNA ENKRIPCIJA

⇒ ovaj dio „kvantne informacije" se intenzivno koristi

⇒ ovo nije nikakva enkripcija, nego je to samo protokol za razmjenu tajnog ključa

↳ sama enkripcija je klasična!

QKD = „Quantum Key Distribution"

⇒ <u>dva bitna protokola:</u>

- BB84 (Bennet i Brassard, 1984)
  - ↳ koristi se komplementarnost baza u pripremi i mjerenju stanja bitova
    - ↳ svodi se na rotaciju dvolonca prilikom mjerenja Qbita
- E91 (Eckert, 1991)
  - ↳ oslanja se na spregnuta stanja bitova

(ovime se nećemo sada baviti)

⇒ TERMINOLOGIJA:

- „Alice" - pošiljatelj
- „Bob" - primatelj
- „Eve" - prisluškivatelj
- uspostava se dostavlja ako se primjeti da je ključ bio prisluškivan

⇒ PRETPOSTAVKE:

- Alice može Bobu poslati niz fotona u različitim stanjima linearne polarizacije
- Bob može mjeriti stanje polarizacije fotona (ali ne zna kako ih je Alice poslala)

⇒ između Alice i Bob postoj dogovor (za taj dogovor zna i Eve):

BAZA	POLARIZACIJA	VRIJEDNOST
⊕	↕	0
	↔	1
⊗	↗	0
	↖	1

↳ no Bob ne zna je l Alice slala nule il jedinice niti koju je bazu koristila

- Alice šalje random 0, 1 u random bazi
- Bob random okreće bazu i mjeri niz primljenih fotona
- Bob objavljuje svoje baze korištene u mjerenju te mu Alice javlja na kojim mjestima su baze dobro odabrane (time Alice objavljuje i svoje odabrane baze, no sada je to kasno za Eve jer su te fotoni izmjereni i zna ih samo Bob)
- stoga, Bob koristi samo mjesta ključa gdje su baze dobro odabrane

⇒ na kraju, Bob i Alice usporeduju svoje ključeve na 25% mjesta gdje su bare dobro odabrane

↳ ako se utvrdi varljka na jednom mjestu, ključevi nisu dobri i treba se generirati sve iz početka

↳ ako se utvrdi jednakost ključeva, komunikacija nije bila prisluškivana i sigurni smo da možemo koristiti cijele ključeve za dekripciju poruka (samo 25% ključa je bilo javno objavljeno)

MATRIČNI ZAPIS STANJA I OPERATORA

⇒ vektore ortonormirane baze $\{|0\rangle, |1\rangle\}$ u $\mathcal{H}^2$ možemo prikazat vektor-stupcima:

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

⇒ bilo koj vektor se može izrazit ovako:

$$\boxed{|\phi\rangle = \lambda \cdot |0\rangle + \mu |1\rangle = \begin{pmatrix} \lambda \\ \mu \end{pmatrix}}$$

⇒ dualni vektor je tada:

$$\langle \phi | = \lambda^* \langle 0| + \mu^* \langle 1| = \begin{pmatrix} \lambda^* & \mu^* \end{pmatrix}$$

⇒ <u>skalarni produkt</u>:

$$|\phi\rangle = \begin{pmatrix} \lambda \\ \mu \end{pmatrix} \qquad |\psi\rangle = \begin{pmatrix} \nu \\ \sigma \end{pmatrix}$$

$$\langle \psi | \phi \rangle = \begin{pmatrix} \nu^* & \sigma^* \end{pmatrix} \cdot \begin{pmatrix} \lambda \\ \mu \end{pmatrix} = \nu^* \lambda + \sigma^* \mu$$

⇒ <u>hermitski operator</u>:

- u matričnoj reprezentaciji, to je dijagonalna matrica sa vrijednostima „a_n" na dijagonali
  ↳ ovo vrijedi za ortonormiranu bazu!

• na općenitu bar to više nije tako nego se elementi rasporede po cijeloj matrici, dijagonala je realna, a vrijedi kompleksno - konjugirana simetrija

↳ to znači da svaki hermitski operator možemo prikazat u nekoj bazi u kojoj je on dijagonalan sa svojstvenim vrijednostima na dijagonali:

$$(M)_{\alpha\beta} = \langle \alpha | M | \beta \rangle = \langle \alpha | I | M | I | \beta \rangle = \sum_m |m\rangle\langle m|$$

$$= \left\langle \alpha \left| \sum_m |m\rangle\langle m| \; M \; \sum_n |n\rangle\langle n| \right| \beta \right\rangle =$$

$$= \sum_{m,n} \langle \alpha | m \rangle \underbrace{\langle m | M | n \rangle}_{a_n \delta_{mn}} \langle n | \beta \rangle = (*)$$

↳ uzeo se da je ovo gore sve nula, samo je nešto smisleno kada je $m = n$

$$(*) = \sum_n \langle \alpha | n \rangle a_n \langle n | \beta \rangle =$$

$$= \sum_n \langle n | \alpha \rangle^* a_n \langle \beta | n \rangle^*$$

$$= \left(\sum_n \langle \beta | n \rangle a_n \langle n | \alpha \rangle \right)^* = \left(M_{\beta\alpha} \right)^*$$

⇒ **OPĆENITO STANJE QBITA:**

$$|\phi\rangle = e^{-i\frac{\delta}{2}} \cos\left(\frac{\vartheta}{2}\right)|0\rangle + e^{i\frac{\delta}{2}} \sin\left(\frac{\vartheta}{2}\right)|1\rangle$$

⬇

ovo je Blochova sfera

↳ suprotnost u 3D prostoru je ekvivalencija okomitosti u Hilbertovom prostoru

↳ općenito stanje je superpozicija bilo koja dva proizvoljno izabrana stanja

↳ imena osi u Blochovoj sferi nemaju veze sa smjerovima polarizacije fotona, pa nemoj to pomiješat !

⇒ PAULIJEVE MATRICE:

↳ projektori na vektore stanja:

a) vektor stanja $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

↳ projektor $|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

b) vektor stanja $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

↳ projektor $|1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

↳ koristeći projektore sastavljamo važan hermitski operator:

$$\sigma_z = (+1)\,|0\rangle\langle 0| + (-1)\,|1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

↳ slično, sastavljamo i hermitske operatore na točke u stanjima na ostale osi:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

↳ nekad se koriste indeksi 1, 2, 3 umjesto oznake osi:

$$\sigma_x = \sigma_1 \qquad \sigma_y = \sigma_2 \qquad \sigma_z = \sigma_3$$

⬇

te matrice odgovaraju
svojstvenim vrijednostima stanjima
na osi te se nazivaju
Paulijeve matrice

⇒ Paulijeve matrice su korisne jer preko njih mogu rapisati bilo koj hermitski operator:

$$M = \lambda_0 I + \sum_{i=1}^{3} \lambda_i \sigma_i$$

$\lambda_j \in R$; $j = 0, 1, 2, 3$

⇒ UKRATKO O SPINU:

- spin je svojstvo čestica koje nam može poslužit za za kalibraciju Qbita
- spin je temeljno svojstvo uz masu i električni naboj
- spin je u prirodi kvantiziran:

$$s = 0, \frac{1}{2}, 1, \frac{3}{2}, \dots$$

↖ spinski kvantni broj

- sama vrijednost spina je:

$$S = \hbar \sqrt{s(s+1)}$$

- spin se može izmjeriti samo tako da se odlučimo za jednu os i možemo izmjeriti projekciju spina na tu os

⇒ čestice spinskog kvantnog broja $s = \frac{1}{2}$, moguće je samo projecirat spin na z-os na dva načina:

$$S = \pm \frac{\hbar}{2}$$

↳ zbog toga što ovo ima samo dva načina, ovo je moguća realizacija Qbita

↳ stoga, projekciju spina na x, y i z možemo zapisat hermitskim operatorima:

$$S_x = \frac{\hbar}{2}\sigma_1 \qquad S_y = \frac{\hbar}{2}\sigma_2 \qquad S_z = \frac{\hbar}{2}\sigma_3$$

$$\vec{S} = \frac{\hbar}{2}\vec{\sigma} \longrightarrow \text{vektorski zapis}$$

SUSTAV DVAJU QBITOVA

⇒ bitan pojam ovdje je **SPREGNUTOST** (engl. „entanglement")
↳ kod sustava jednog Qbita, moglo bi nas pojam je **superpozicija**

⇒ no, prvo se moramo upoznati sa ostalim bitnim pojmovima

⇒ stanje Qbita A pribacujemo vektorom $|\phi_A\rangle$ u Hilbertovom prostoru H_A koristeći ortonormiranu bazu $\{|0_A\rangle, |1_A\rangle\}$
↳ analogno za Qbit B
↳ **TENZORSKI PRODUKT:**
- stanje sustava koji se sastoji od tih dvaju Qbita
- pišemo: $|\phi_A\rangle \otimes |\phi_B\rangle$ il $|\phi_A \otimes \phi_B\rangle$

⇒ prirodno se nameće odabir baze koja je ortonormirana:

$$\{ |ij\rangle = |i_A \otimes j_B\rangle \; ; \; i,j = 0,1 \}$$

$$\{ |00\rangle = |0_A \otimes 0_B\rangle$$
$$|01\rangle = |0_A \otimes 1_B\rangle$$
$$|10\rangle = |1_A \otimes 0_B\rangle$$
$$|11\rangle = |1_A \otimes 1_B\rangle \}$$

⇒ općenit vektor u takvom prostoru ⇔ takvom bazom:

$$|\Phi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

$$\alpha, \beta, \gamma, \delta \in \mathbb{C}$$

⇒ O OPERATORIMA:

- ako imamo dva „jedno-Qbitna" operatora M_A i M_B koj djeluju na svoje Qbitove, njihovo djelovanje u prostoru $H_A \otimes H_B$ jest tenzorski produkt tih operatora:

$$M_A \otimes M_B$$

↳ stoga, ako želimo projecirati spina prve čestice (Qbit A) na Z-os, a drugu česticu nas ne zanima, u prostoru $H_A \otimes H_B$ koristimo „dvo-Qbitni" operator

$$\frac{\hbar}{2}\sigma_z \otimes I$$

↓

„ignoriraj drugu česticu"

⇒ matrični prikaz ortonormirane baze:

$$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \quad |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \quad |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \quad |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

⇒ matrični prikaz bilo kojeg vektora:

$$|\Phi\rangle = \begin{bmatrix}\alpha\\\beta\\\gamma\\\delta\end{bmatrix}$$

⇒ još trebamo matrični zapis operatora:

↳ PAZI!! Notacija indeksiranja je malo zbunjujuća jer indeksi nisu indeksi pozicije u matrici nego su prikaz stanja koje se reprezentira:

$$A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}$$

$$a_{00} = \langle 0|A|0\rangle$$
$$a_{01} = \langle 0|A|1\rangle$$
$$a_{10} = \langle 1|A|0\rangle$$
$$a_{11} = \langle 1|A|1\rangle$$

PR: Prikaz tenzorskog operatora u matričnom obliku!

$$M_A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad M_B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

$$M_A \otimes M_B = \begin{pmatrix} a M_B & b M_B \\ c M_B & d M_B \end{pmatrix}$$

$$M_A \otimes M_B = \begin{pmatrix} a\alpha & a\beta & b\alpha & b\beta \\ a\gamma & a\delta & b\gamma & b\delta \\ c\alpha & c\beta & d\alpha & d\beta \\ c\gamma & c\delta & d\gamma & d\delta \end{pmatrix}$$

⇒ vremenska evolucija kvantno-mehaničkog sustava mora biti opisana <u>unitarnim operatorima</u>

↳ to su operatori koji čuvaju stanje sustava

↳ ako stanje nije očuvano, takav sustav nije moguće izvesti (ne postoji), pa trebamo probati drugačiji algoritam, tj. na drugačiji način probati napisati algoritam kvantnog računala

⇒ **SEPARABILNA I SPREGNUTA STANJA:**

↳ bitna svojstva sustava dvaju Qbita

↳ Qbitovi su u stanjima:

$$|\Phi_A\rangle = \lambda_A |0_A\rangle + \mu_A |1_A\rangle$$

$$|\Phi_B\rangle = \lambda_B |0_B\rangle + \mu_B |1_B\rangle$$

↳ stanje sustava prikazujemo vektorom stanja:

$$|\Phi\rangle = |\Phi_A \otimes \Phi_B\rangle$$

$$|\Phi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

⇓ slijedi

$$\alpha = \lambda_A \lambda_B$$
$$\beta = \lambda_A \mu_B$$
$$\gamma = \mu_A \lambda_B$$
$$\delta = \mu_A \mu_B$$

iz toga, uočavamo da vrijedi:

$$\alpha\delta = \beta\gamma$$

⇓

to znači da tenzorski produkt $|\Phi_A \otimes \Phi_B\rangle$ ne predstavlja potpuno općenit vektor stanja (mora vrijediti $\alpha\delta = \beta\gamma$)

BITNO!

stoga, tenzorski produkt je dosta ⟸ bogati operator (nosi puno informacije)

↳ stoga, tenzorski produkt vektorskih vektora stanja dvaju Qbitova nesto je podskupa rezultata koje dozvoljava opcenitti tenzorski produkt u Hilbertovom prostoru

↳ SEPARABILNA STANJA:

- stanja dvaju il vise Qbitova koja je moguće prikazati tenzorskim produktom vektora stanja pojedinih Qbitova

↳ SPREGNUTA STANJA:

- stanja u kojem sustav dva il vise Qbitova nije moguće prikazat tenzorskim produktom vektora stanja pojedinih Qbitova
- tu je bogatstvo informacije

⇒ superpozicija i spregnutost su glavni pojmovi i oni su razlog za bogatstvo informacije Qbita

⇒ primjer spregnutog stanja vise Qbita:

$$|\Phi\rangle = 1|00\rangle + 2|01\rangle + 3|10\rangle + 4|11\rangle$$

↓

ne možemo prikazat tenzorskim produktom stanja Qubita jer $LS \neq PS$

PR: Promatramo sustav dvaju qubita A i B koji se nalaze u spregnutom stanju:

$$|\Phi\rangle = \frac{1}{\sqrt{2}} \left(|0_A \otimes 1_B\rangle + |1_A \otimes 0_B\rangle \right)$$

⇒ primijenimo operator koji opisuje fizikalnu veličinu povezanu s qubitom A:

$$M \otimes I$$

↳ samo radi nešto s qubitom A
(M je pravilan operator na prvi qbit, a I na drugi)

$$\underbrace{\langle \Phi | (M \otimes I) | \Phi \rangle}_{\text{OČEKIVANA VRIJEDNOST U SPREGNUTOM SUSTAVU}} = (*)$$

↳ raspišimo početno spregnuto stanje:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}} |01\rangle + \frac{1}{\sqrt{2}} |10\rangle = \frac{1}{\sqrt{2}} |0_A\rangle \otimes |1_B\rangle + \frac{1}{\sqrt{2}} |1_A\rangle \otimes |0_B\rangle$$

↳ raspišimo operator malo lijepše da se vidi djelovanje:

$$M \otimes I = M_A \otimes I_B$$

$$(*) = \frac{1}{\sqrt{2}} \left(\langle 0_A| \otimes \langle 1_B| + \langle 1_A| \otimes \langle 0_B| \right) \cdot (M_A \otimes I_B) \frac{1}{\sqrt{2}} \left(|0_A\rangle \otimes |1_B\rangle + |1_A\rangle \otimes |0_B\rangle \right) =$$

$$= \frac{1}{\sqrt{2}} \left(\langle 0_A| \otimes \langle 1_B| + \langle 1_A| \otimes \langle 0_B| \right) \cdot \frac{1}{\sqrt{2}} \left(|M_A 0_A\rangle \otimes |1_B\rangle + |M_A 1_A\rangle \otimes |0_B\rangle \right) =$$

$$= \frac{1}{2} \underbrace{\langle 0_A | M_A 0_A \rangle}_{\text{očekivana vrijednost kada je qbit u stanju 0}} + \frac{1}{2} \underbrace{\langle 1_A | M_A 1_A \rangle}_{\text{očekivana vrijednost kada je qbit u stanju 1}}$$

OKRENI ▽

↳ operatorom $M \otimes I$ ignoriramo drugi Qbit, pa logično očekujemo da ako izračunamo očekivanu vrijednost samo prvog Qubita, dobivamo istu vrijednost: (no, razuvjerit ćemo se!)

$$|\Phi_A\rangle = \lambda_A |0_A\rangle + \mu_A |1_A\rangle$$

$$\langle \Phi_A | M_A | \Phi_A \rangle = \left(\lambda_A^* \langle 0_A| + \mu_A^* \langle 1_A| \right) M_A \left(\lambda_A |0_A\rangle + \mu_A |1_A\rangle \right) =$$

$$= |\lambda_A|^2 \langle 0_A | M_A 0_A \rangle + |\mu_A|^2 \langle 1_A | M_A 1_A \rangle +$$
$$+ \lambda_A^* \mu_A \langle 0_A | M_A 1_A \rangle + \mu_A^* \lambda_A \langle 1_A | M_A 0_A \rangle$$

↓

nismo dobili isto!

↳ to je zbog spregnutosti; pa čim jedan qbit gledamo razdvojeno, to više nije taj qbit!

↳ da se početno sustav Qbita nalazio u separabilnom stanju, dobili bi isti rezultat, no ovdje to nije slučaj!

BITNO!

⇒ NAPOMENA:

↳ bitne oznake: $|\Phi_+\rangle = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle)$

$|\Phi_-\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$

⇒ VAŽNA SPOZNAJA:

↳ primjer na slajdovima s vremenskom ovisnosti kvantnog sustava pokazuje da sustav prelazi iz separabilnog stanja u spregnuto i obratno tijekom vremena, i to spontano (bez vanjskih poluda)

↳ to dobijemo rješavanjem Schrödingerove jednadžbe za sustav dva Qubita

↳ to nam govori da iako nam je lakše razumjeti sustav Qubita u separabilnom stanju, ne možemo se služit sustavom koji je u separabilnom stanju jer će on ubrzo prijeći u spregnuto, nakon u separabilno, itd.

⇒ **OPERATOR STANJA:** (matrica gustoće)

↳ služi za opis sustava koji se sastoji od dva podsustava A i B unutar kojih koristimo ortonormirane baze $\{|i\rangle\}$ i $\{|\mu\rangle\}$:

$$|\Phi\rangle = \sum_{i,\mu} c_{i\mu} |i \otimes \mu|$$

↳ drugim riječima, ako imamo (na primjer) dva Qubita, ne možemo više jedan Qubit gledati zasebno i prikazati njegovo stanje samo kvantima, pa trebamo novi operator

↳ to je **operator stanja**

PRIMJERI OPERACIJA

⇒ ako želimo zbroj spinova dviju čestica na Z-os, radimo sljedeće:

$$\sigma_Z \otimes I + I \otimes \sigma_Z$$

⇒ ako želimo energiju, to je skalarni produkt projekcija na Z-os, radimo sljedeće:

$$\sigma_Z \otimes \sigma_Z$$

⇒ <u>swap operator</u>:

↳ zanimljiv je fizikalno i računski jer se vidi što radi: $M_{swap}|ij\rangle = |ji\rangle$

↳ izvod swap operatora:

$$M_{swap} = I + \vec{\sigma}_A \cdot \vec{\sigma}_B$$

$$= I + (\vec{i}\sigma_{XA} + \vec{j}\sigma_{YA} + \vec{z}\sigma_{ZA}) \cdot (\vec{i}\sigma_{XB} + \vec{j}\sigma_{YB} + \vec{z}\sigma_{ZB}) = (*)$$

„σ_A i σ_B nisu iz istog prostora, pa unijeste klasičnog prostora koristi tenzorski produkt"

$$(*) = I + \sigma_{XA} \otimes \sigma_{XB} + \sigma_{YA} \otimes \sigma_{YB} + \sigma_{ZA} \otimes \sigma_{ZB}$$

bilo što modula 1

⇒ <u>NAPOMENA</u>:

↳ stanje $|\Psi\rangle$ i $e^{i\phi}|\Psi\rangle$ su ista stanja

↳ $|\Psi\rangle$ je u tom slučaju stanje kvantnog sustava (a ne samo jednog Qubita, ako se radi o sustavu više Qubita)

DODATNO O SPREGNUTIM STANJIMA

⇒ rekl smo da jedan Qubit u sustavu više Qbita ne možemo prikazat (u općenitosti) samog pomoću njegovih ketova

↳ to je zbog spregnutosti i trebamo koristit operator stanja!

PRB Želimo opisat podsustav A u stanju koje je možda spregnuto sa podsustavom B!

↳ trebamo izračunat operatora M_A:

$$\langle \Phi | (M_A \otimes I_B) | \Phi \rangle = \ldots = \sum_{ij} \mathcal{S}_{ij} M_{ji} = Tr(\mathcal{S}_A M_A)$$

↳ gdje je $\mathcal{S}_A$ operator čiji su matrični elementi:

$$(\mathcal{S}_A)_{ij} = \mathcal{S}^A_{ij} = \sum_{\mu} \alpha_{i\mu} \alpha^*_{j\mu}$$

$\mathcal{S}_A \Rightarrow$ reducirani operator stanja podsustava A

CIJELI IZVOD:

$$\langle \Phi | M_A \otimes I_B | \Phi \rangle = \left(\sum_{j\nu} \alpha^*_{j\nu} \langle j \otimes \nu | \right) (M_A \otimes I_B) \left(\sum_{i,\mu} \alpha_{i\mu} | i \otimes \mu \rangle \right) =$$

$$= \sum_{j,\nu,i,\mu} \alpha^*_{j\nu} \alpha_{i\mu} \langle j \otimes \nu | M_A \otimes I_B | i \otimes \mu \rangle = (*)$$

OKREMO

↳ koristimo grčke i latinske indekse s razlogom da si uljepšamo prikaz:

- jedni simbol su za jedan Qbit, a drugi za drugi Qbit
- samim time, djelovanje operatora na drugi Qbit, daje nulu

$$(*) = \sum_{j,\nu,i,\mu} \mathcal{L}^*_{j\nu} \mathcal{L}_{i\mu} \langle j \otimes \nu | M_A \, i \otimes \mu \rangle =$$

$$= \sum_{j,\nu,i,\mu} \mathcal{L}^*_{j\nu} \mathcal{L}_{i\mu} \langle j | M_A | i \rangle \delta_{\nu\mu} =$$ „uklanjamo sumu po „ν"

$$= \sum_{j,i,\mu} \mathcal{L}^*_{j\nu} \mathcal{L}_{i\mu} \langle j | M_A | i \rangle =$$

$$= \sum_{i,j} \boxed{\sum_{\mu} (\mathcal{L}_{i\mu} \mathcal{L}^*_{j\nu})} (M_A)_{ji} = (*)$$

ovo ima strukturu matrice, to je operator $\mathcal{S}_A$

$$(*) = \boxed{\sum_{i,j} (\mathcal{S}_A)_{ij} (M_A)_{ji}} = (*)$$

primjeti da je ovo zapravo matrično množenje:

$$\sum_j a_{ij} b_{jk} = C_{ik}$$

sa „j" dobijemo matricu, a sa i sumiramo elemente po matrici:

- to se naziva **Trace** (oznaka Tr)

$$(*) = \sum_i (\mathcal{S}_A \cdot M_A)_{ii} = \mathrm{Tr}(\mathcal{S}_A \cdot M_A)$$

⇒ PONOVIMO:

- vektorom u Hilbertovom prostoru možemo prikazati samo cijel kvantni sustav
  - ↳ to može biti jedan Qbit ili više Qbita
- znači, jedan Qbit, ako je sam u kvantnom sustavu, možemo prikazati u nekom stanju vektorom u Hilbertovom prostoru (njegovim ketovima)
  - ↳ ako se radi o sustavu više Qbita, moramo koristiti operator stanja da bi prikazali stanje pojedinog Qbita
- <u>stoga, zaključak:</u>
  - ↳ operatorom uvijek možemo prikazati stanje Qbita dok vektorom to ne možemo uvijek zbog spregnutosti stanja

⇒ NAPOMENA:

- za ispit isprintaj ρ_A i ρ_B za sustav dva Qbita!
  - ↳ nalazi se na primjeru nakon izvoda za operator stanja

zbroja se u 1 i moraju biti pozitivni!

ZAD: Neka je: $\mathcal{S}_A = \begin{pmatrix} \frac{1}{2} & -\frac{i}{2} \\ \frac{i}{2} & \frac{1}{2} \end{pmatrix}$

Odredi kojem od stanja Qbita odgovara gore napisani reduciran operator stanja A!

↳ Qbit A je u stanju:

$$|\phi\rangle = \lambda_A |0\rangle + \mu_A |1\rangle$$

↳ sustav (AB) je u separabilnom stanju jer možemo prikazat A u stanju (to se traži) pomoću ketova!

$$\mathcal{S}_A = \begin{pmatrix} \frac{1}{2} & -\frac{i}{2} \\ \frac{i}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} |\lambda_A|^2 & \lambda_A \mu_A^* \\ \lambda_A^* \mu_A & |\mu_A|^2 \end{pmatrix}$$

$$\Downarrow$$

slijed: $|\lambda_A| = \frac{1}{\sqrt{2}} \Rightarrow$ pretpostavimo: $\lambda_A = \frac{1}{\sqrt{2}}$

$$|\mu_A| = \frac{1}{\sqrt{2}}$$

$$\frac{1}{\sqrt{2}} \mu_A^* = -\frac{i}{2} \Rightarrow \mu_A = \frac{i}{\sqrt{2}}$$

↳ stoga, dobil smo jednoznačan prikaz stanja Qbita do na fazu:

$$|\phi_A\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + i |1\rangle \right)$$

⇒ NAPOMENA:

· ako i samo ako vrijedi $\hat{\rho}^2 = \hat{\rho}$, sustav je u **čistom stanju**

⇒ iz svojstva operatora $\hat{S}_A$ slijedi da je moguće pronaći bazu $\{|i\rangle\}$ u kojoj on ima oblik:

$$\hat{S}_A = \sum_i p_i^A |i\rangle\langle i|$$

p_i^A ⇒ operator „$\hat{S}_A$" pridružuje mjerljivoj stanja u kojoj su stanja $|i\rangle$ prisutna sa vjerojatnošću „p_i"

↳ pogledajmo, radi li se tada o čistom stanju:

$$(\hat{S}_A)^2 = \hat{S}_A \hat{S}_A = \left(\sum_j p_j^A |j\rangle\langle j|\right)\left(\sum_i p_i^A |i\rangle\langle i|\right) =$$

$$= \sum_{i,j} p_i^A p_j^A |j\rangle\langle j|i\rangle\langle i| = (*)$$

$\langle j|i\rangle$ → δ_{ij} (različite od nule samo kada su jednake, pa možemo shvatiti kao jediničnu matricu)

$$(*) = \sum_i p_i^A p_i^A |i\rangle\langle i| = \sum_i (p_i^A)^2 |i\rangle\langle i|$$

, ova vrijedi ako su sve vjerojatnosti nula osim jedne koja je jedan!

⇒ TEOREM O NEMOGUĆNOSTI KVANTNOG KLONIRANJA:

- kloniranje se smatra transformacija koja stanje jednog Qbita prenos na drugi Qbit:

$$|\chi \otimes \phi\rangle \rightarrow |\chi \otimes \chi\rangle$$

- ne postoj unitarni operator koj to može napravit, pa smatramo da je to nemoguće
- ovaj teorem objašnjava zašto Eve ne može prisluškivat komunikaciju između Bob i Alice bez da izmjeni informaciju
- dokaz se bazira na kontradikciji
  ↳ pretpostavimo da postoj unitarni operator koj može klonirat
  (nećemo radit dokaz :))

⇒ EINSTEIN - PODOLSKY - ROSENOV PARADOKS:

↳ Alice mjeri Σ-os, a Bob mjeri Y

↳ znamo da Alice mjeri negativno od Bola i time Alice i Bob (ako se čuju telefonom) mogu znati sve o Alici - oba su uspješno izmjerili svoju os i javili su drugom

· kako sad oba mogu znati sve o Alici pomoću mjerenja svoje osi?

↳ tu se ruši zamisao i upitna postoje interpretacija kvantne mehanike jer pokus na jednom kraju svemira utječe na pokus na drugom kraju svemira

⇓

moderni odgovor na to je da nema paradoksa jer Alice i Bob možda ne mjere istu čestica (svemir se ne sastoji samo od jedne čestice)

(ovo je rezultat spregnutosti)

KLASIČNO RAČUNALO

⇒ stanja klasičnog bita možemo prikazati vektor-stupcima:

$$0 \leftrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad 1 \leftrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

⇒ stanja dva klasična bita možemo prikazati ovako:

$$00 \leftrightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad 01 \leftrightarrow \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad 10 \leftrightarrow \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad 11 \leftrightarrow \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

↳ stoga, u prikazu stanja klasičnog računala pomoću vektor-stupca trebamo 2^N članova u tom stupcu

↳ ovo je dakle dulji zapis, ali omogućuje da djelovanje logičkih vrata zapisujemo u matričnom obliku:

$$\left.\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\right\} \text{prikaz „and" operatora}$$

⇓

ovo je zapravo tablica istinitosti:

AND	00	01	10	11
0	1	1	1	0
1	0	0	0	1

⇒ u digitalnoj logici znamo da za proizvoljno složena logička vrata trebamo samo dvoja vrata: NOT i AND (il OR)

↳ ako baš želimo, mogu nam čak biti dovoljna i samo jedna vrata: NAND

⇒ DE MORGANOV IDENTITET:

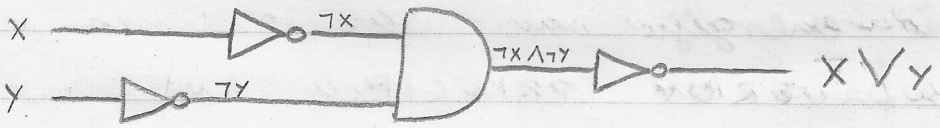
↳ u ovoj notaciji zapisujemo ga ovako:

$$x \vee y = \neg(\neg x \wedge \neg y)$$

↳ matričan prikaz:

$$OR = NOT \cdot AND \cdot (I \otimes NOT) \cdot (NOT \otimes I)$$

↳ inverzija ovo u matričnom prikazu!



⇒ klasična digitalna logika (digitalna vrata) nisu reverzibilna:

- jednom kada podaci prođu kroz AND/OR vrata, više ne možemo znati što je bilo na ulazu, pa entropija raste (neka informacija je poništena, pa to implicira povećanje entropije - ako se entropija povećala, termodinamika govori da se „troši" energija (oslobađa se toplina)) BITNO!

⇒ stoga, krenulo se u istraživanje:

- pošto se energija troši na uništavanje informacije, pa možemo li načiniti takvo računalo / sustav koji je neće uništavati?

↳ u prošlom poglavlju smo se upoznali s 3. principom kvantne mehanike, i vidjeli smo da je **vremenska evolucija kvantnog sustava opisana unitarnim operatorima** (to su operatori koji čuvaju stanje sustava, a time i informaciju i energiju)

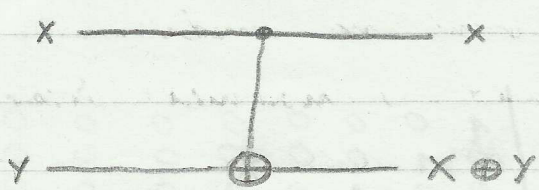
⇒ eksperimentalno je pokazano da da gubljenje informacije troši energiju

↳ LANDAUEROV PRINCIP

(on je pokrenuo razmišljanje o povezanosti informacije i energije tako da je povezao Shannonovu teoriju i termodinamiku)

⇒ CONTROL-NOT VRATA:

„X" ⇒ kontrolni bit



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

↳ matrični prikaz je uvijek kvadratna matrica kako bi bio reverzibilan

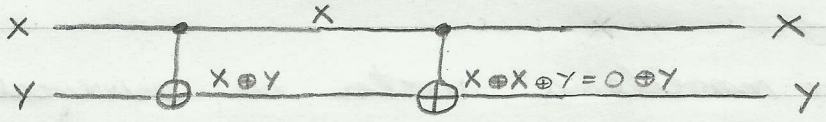
↳ dokaz reverzibilnosti:

$$cNOT \cdot cNOT = I$$

(sam sebi je inverz)

} matrični dokaz

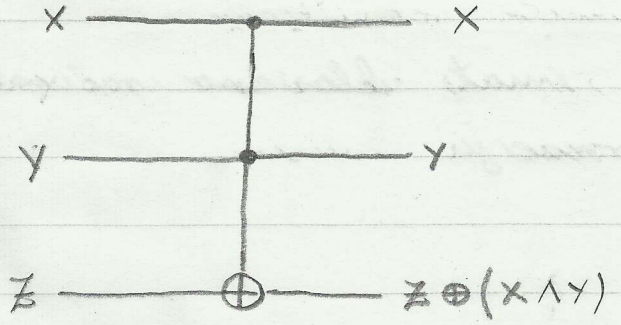
↳ reverzibilnost na slici:



} slikovni dokaz

⇒ TOFFOLIJEVA VRATA:

„X" i „Y" ⇒ kontrolni bitovi

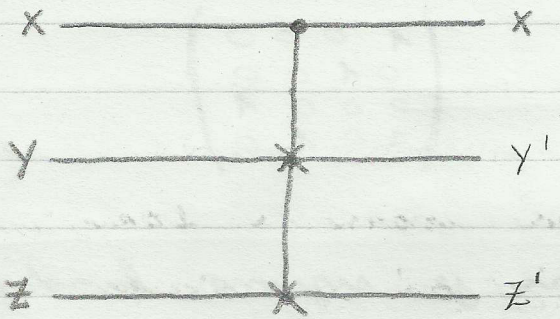


$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

↳ nije teško pokazati reverzibilnost na sličan način kao i kod cNOT vrata

⇒ **FREDKINOVA VRATA**

„X" ⇒ kontrolni bit



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

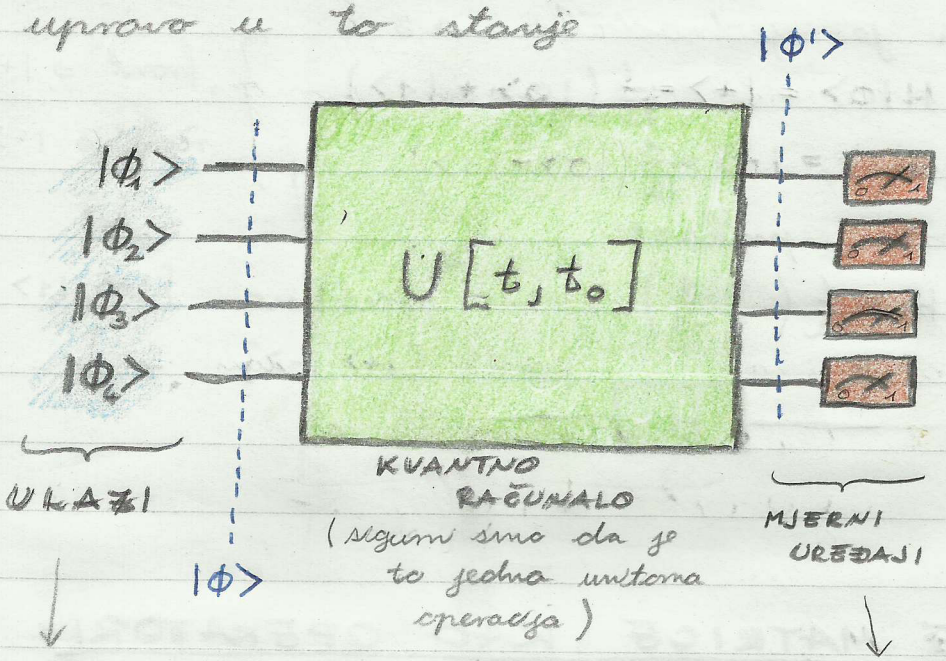
↳ reverzibilnost dokazujemo na iste načine kao i kod prethodnih vrata

⇒ sva od tri navedena vrata su univerzalna što znači da s njima možemo napraviti sve proizvoljno - kompliciranе logičke sklopove (dokazujemo take da ostvarimo NAND sklop il AND i NOT il OR i NOT)

↳ stoga, možemo imati klasično računalo koje ne gubi informaciju

KVANTNO RAČUNALO

⇒ može se naći u beskonačnom mnoštvu stanja (superpozicija 2^N stanja računalne bare), a mjerenjem se dobiva neko od 2^N stanja računalne bare, a samo računalo prelazi upravo u to stanje



neki foton ili spinovi dovedeni u željeno stanje i pušteni u kvantno računalo

ne znamo je li sustav u separabilnom ili spregnutom stanju (svaki od njih može poprimati 0 ili 1, pa imamo 2^4 mogućih izlaza - sve bogatstvo kvantnog svojeta se gubi prilikom tog mjerenja (služi samo za račun))

⇒ sada ćemo pogledat unutrošnjost kvantnog računala - zanimaju nas operatori (vrata) koji mogu djelovat <u>na 1 Qbit</u> (SVI MORAJU BITI UNITARNI)

⇒ <u>HADAMARDOV OPERATOR:</u>

↳ djeluje na jedan Qbit

↳ svojstvo $H^2 = I$ pokazuje unitarnost

↳ dan je jednadžbama:

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

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

„front" ⇒ $|+\rangle$

„rear" ⇒ $|-\rangle$

↳ matrični prikaz:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

⇒ preslikava $\{|0\rangle, |1\rangle\}$ u $\{|+\rangle, |-\rangle\}$



⇒ <u>PAULIJEVE MATRICE KAO OPERATORI:</u>

↳ matrice σ_x, σ_y i σ_z su također dobri operatori za rad s jednim Qbitom

⇒ <u>DODATNI OPERATORI:</u>

↳ vidi matrice „S" i „T" na slajdovima te se uvjeri da one dobro rade s jednim Qubitom

⇒ trebaju nam i operatori koji mogu djelovat na **više Qbita** (SVI MORAJU BITI UNITARNI)

⇒ **VRATA cNOT:**

↳ preuzmamo ih iz klasične logike

↳ ako se stanja $|x\rangle$ i $|y\rangle$ qubitova sa vektorima baze $\{|0\rangle, |1\rangle\}$, djelovanje cNOT vrata očituje se ovako:

$$|x\rangle \otimes |y\rangle \longrightarrow |x\rangle \otimes |x \oplus y\rangle$$

(specijalni slučaj)

⇒ u teoriji / načelu, svi algoritmi koji se mogu izvesti na klasičnom računalu se mogu izvesti i na kvantnom (iako, u praksi to baš nije tako jer nemamo jako puno Qbita)

BITNO!

PR: Pogledajmo operator s navedenim preslikavanjem i provjerimo je li to unitaran operator (da li svakom stanju čuva normu)?

$$M|0\rangle = |0\rangle$$
$$M|1\rangle = |0\rangle$$

prvi stupac: $\begin{pmatrix} & \\ & \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

drugi stupac: $\begin{pmatrix} & \\ & \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

↳ iz toga iščitavamo:

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

↳ odmah vidimo da nije jer su jedina dva invertibilna operatora na jednom Qbitu:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

↳ no, provjerimo to na način da dokažemo da M nije invertibilan, tj. da ne vrijedi $M^\dagger M = I$:

$M^\dagger$ ⇒ hermitska konjugacija (transponiraj + kompleksno konjugiraj)

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

⇓ nije identitet, pa nije unitaran

PR: Podsjetimo se, za vježbu, kako provjerit svojstvene vrijednosti i svojstvene vektore na brz način!

↳ ako znamo kako je neki operator konstruiran (definiran) možemo lagano tako da pomnožimo sa $|0\rangle$ i $|1\rangle$:

· npr. $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$

↳ pomnožimo sa $|0\rangle$:

· dobijemo $\sigma_z |0\rangle = |0\rangle$

(jedna svojstveni vektor je $|0\rangle$ sa vrijednosti 1)

↳ pomnožimo sa $|1\rangle$:

· dobijemo $\sigma_z |1\rangle = -|1\rangle$

(druga svojstvena vrijednost je -1 i vektor $|1\rangle$

↳ školski način (ako ne znamo kako je operator načinjen):
(sada za σ_x, a gore je σ_z)

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

$$\sigma_x u = \lambda u$$

$$\underbrace{(\sigma_x - \lambda I)}\, u = 0$$

$$\det[\sigma_x - \lambda I] = 0$$

$$\det\left[\begin{pmatrix} \lambda & 1 \\ 1 & \lambda \end{pmatrix}\right] = 0$$

$$\lambda^2 - 1 = 0 \Rightarrow \lambda_{1,2} = \pm 1$$

(sada imamo vrijednost, ali još trebamo vektore)

$$\sigma_x u_{1,2} = \lambda_{1,2} u_{1,2} = \pm u_{1,2}$$

$$\sigma_x u_1 = u_1 \qquad \sigma_x u_2 = -u_2$$

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

$$\left.\begin{matrix} \mu = \nu \\ \nu = \mu \end{matrix}\right\} u_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad \left.\begin{matrix} \nu = -\mu \\ \mu = -\nu \end{matrix}\right\} u_2 = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

⇒ NAPOMENA:

- matrična reprezentacija hermitskog operatora je otporna na hermitsko konjugiranje (†), što znači da se dobiva ista ta matrica kada ga hermitski konjugiramo
- time su definirane Paulijeve, pa za njih vrijedi:

$$\sigma_x^\dagger = \sigma_x \qquad \sigma_y^\dagger = \sigma_y \qquad \sigma_z^\dagger = \sigma_z$$

- ne moraju sve hermitski operatori biti unitarni (npr. $5|0\rangle\langle 0| = M$
  - $M^\dagger M \neq I$, al je $M^\dagger = M$) //

⇒ vratimo se sada na konsne operatore na jednu Qbit

⇒ **OPERATOR $\sqrt{NOT}$:**

↳ pogledaj na slajdovima i na vježbi provjeri unitarnost i uvjeri se da nije hermitski!

⇒ **OPERATOR FAZNOG POMAKA:**

↳ obavlja rotaciju po paralel Blochove sfere

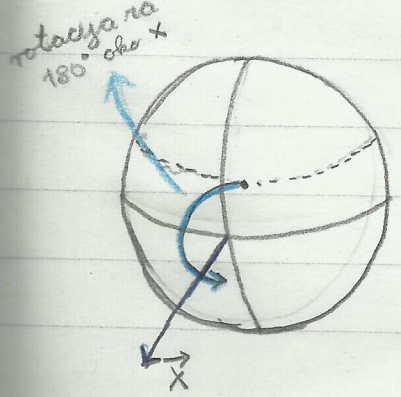
• pokažimo to tako da uzmemo neko općenito stanje $|\psi\rangle = \begin{pmatrix} \cos\frac{\vartheta}{2} \\ e^{i\varphi}\sin\frac{\vartheta}{2} \end{pmatrix}$ i primjenimo operator faznog pomaka:

$$R[\alpha]|\psi\rangle = \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}}_{\text{ovo je operator } R} \begin{pmatrix} \cos\frac{\vartheta}{2} \\ e^{i\varphi}\sin\frac{\vartheta}{2} \end{pmatrix} = \begin{pmatrix} \cos\frac{\vartheta}{2} \\ e^{i(\varphi+\alpha)}\sin\frac{\vartheta}{2} \end{pmatrix}$$

• primjet da Paulijeve matrice napravo rade rotaciju:

a) σ_x rad rotaciju oko x:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad |\psi\rangle = \begin{pmatrix} \cos\frac{\vartheta}{2} \\ e^{-i\frac{\varphi}{2}}\sin\frac{\vartheta}{2} \end{pmatrix}$$



$$\sigma_x|\psi\rangle = \begin{pmatrix} e^{-i\frac{\varphi}{2}}\sin\frac{\vartheta}{2} \\ \cos\frac{\vartheta}{2} \end{pmatrix} = \begin{pmatrix} e^{-i\frac{\varphi}{2}}\cos\left(\frac{\pi}{2}-\frac{\vartheta}{2}\right) \\ \sin\left(\frac{\pi}{2}-\frac{\vartheta}{2}\right) \end{pmatrix}$$

$$= e^{-i\frac{\varphi}{2}} \begin{pmatrix} \cos\frac{\pi-\vartheta}{2} \\ e^{i\frac{\varphi}{2}}\sin\frac{\pi-\vartheta}{2} \end{pmatrix}$$

b) σ_y rad rotaciju oko y

c) σ_z rad rotacija oko z

⇒ TEOREM: općenitu unitarnu transformaciju u $\mathcal{H}^{\otimes n}$ moguće je prikazati kao produkt cNOT vrata i unitarnih transformacija nad pojedinačnim Qbitima

⇒ **VRATA cNOT:**

↳ već smo ih spomenuli ranije

↳ u klasičnoj logici, matrica je:

$$\begin{pmatrix} \boxed{\begin{matrix}1&0\\0&1\end{matrix}} & \boxed{\begin{matrix}0&0\\0&0\end{matrix}} \\ \boxed{\begin{matrix}0&0\\0&0\end{matrix}} & \boxed{\begin{matrix}0&1\\1&0\end{matrix}} \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & \sigma_x \end{pmatrix}$$

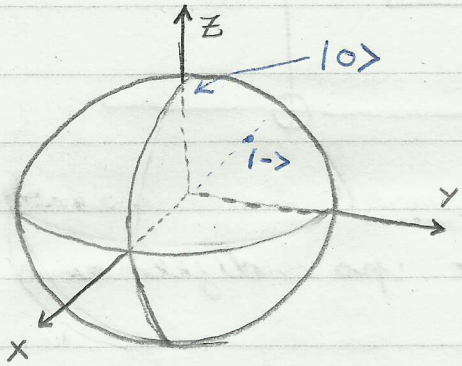
(σ_x je u stvari NOT operator)

⇓
BLOKOVSKI PRIKAZ

↳ napišimo tablicu transformacije u klasičnoj (i kvantnoj) logici:

	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
$\|00\rangle$	1	0	0	0
$\|01\rangle$	0	1	0	0
$\|10\rangle$	0	0	0	1
$\|11\rangle$	0	0	1	0

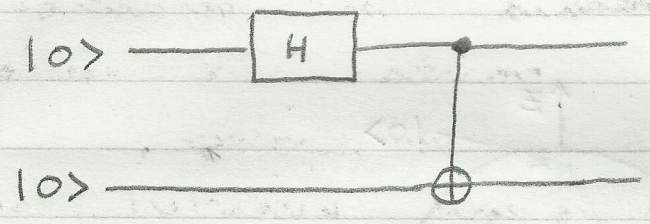
PR: Prisjetimo se Blochove sfere i pokušajmo vidjet sve lijepe osnake za naše algebarske i intuiciju !?



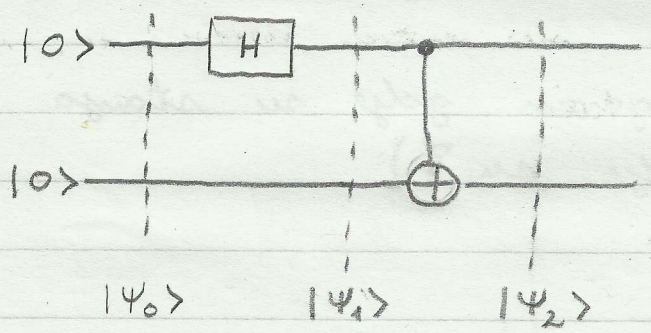
↳ nisam sigurna gdje su stanja |1>, |+>
(pronaći gdje su ?)

ISPIT!? (izvježbaj!)

PR: Neka se sustav dvaju Qbitova nalaz početno u stanju $|\phi\rangle = |0\rangle \otimes |0\rangle = |00\rangle$! Odredimo izlaz sljedećeg logičkog kruga:



↳ raspišimo ovo po dijelovima:



$$|\Psi_0\rangle = |0\rangle \otimes |0\rangle = |00\rangle$$

$$|\Psi_1\rangle = H|0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes |0\rangle$$

separabilno stanje

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

$$|\Psi_2\rangle = cNOT\left[\frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right)\right] = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

spregnuto stanje

(postoji vjerojatnost da izmjerimo $|00\rangle$ il $|11\rangle$ i u ovom slučaju one su jednake)

⇒ primjeti da Hadamardov operator zaprovo Qbit iz baznih stanja baca u spregnuto i na taj način logičk krug s Hadamardovim operatorom računa „dva rezultata" odjednom jer se račun obavlja nad spregnutim stanjima (krug računa u superpoziciji)

↳ to se zove KVANTNI PARALELIZAM i tu se krije moć Hadamardovog operatora

⇒ provedimo račun na istom primjeru, al sada u matričnom obliku:

$$|\psi_0\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|\psi_1\rangle = (H \otimes I)|\psi_0\rangle = \left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) |\psi_0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} I & I \\ I & -I \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|\psi_2\rangle = cNOT|\psi_1\rangle = \begin{pmatrix} I & 0 \\ 0 & \sigma_x \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \frac{1}{\sqrt{2}}$$

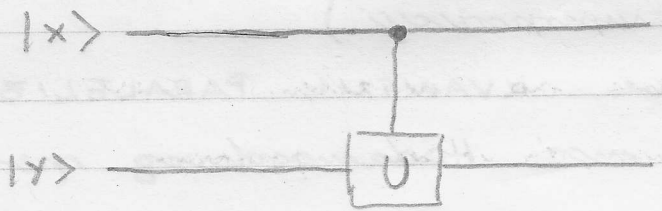
↳ dobil smo isto kao u bra-ket notaciji:

$$|\psi_2\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

⇒ OPERATOR cU

↳ eto, ovo su druga vrata koja nam trebaju (prva su bila cNOT)

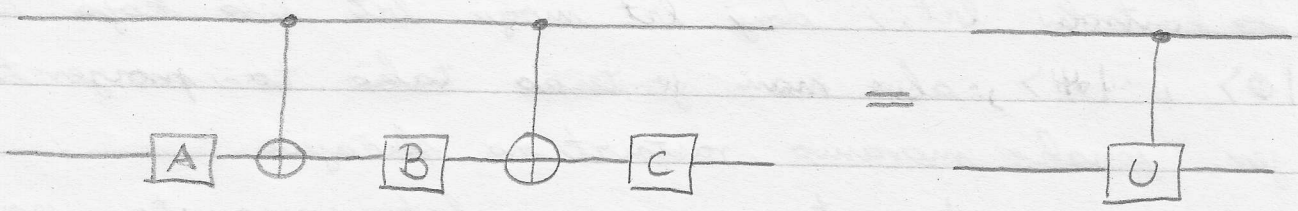
↳ to je sve što treba za kvantno računalo



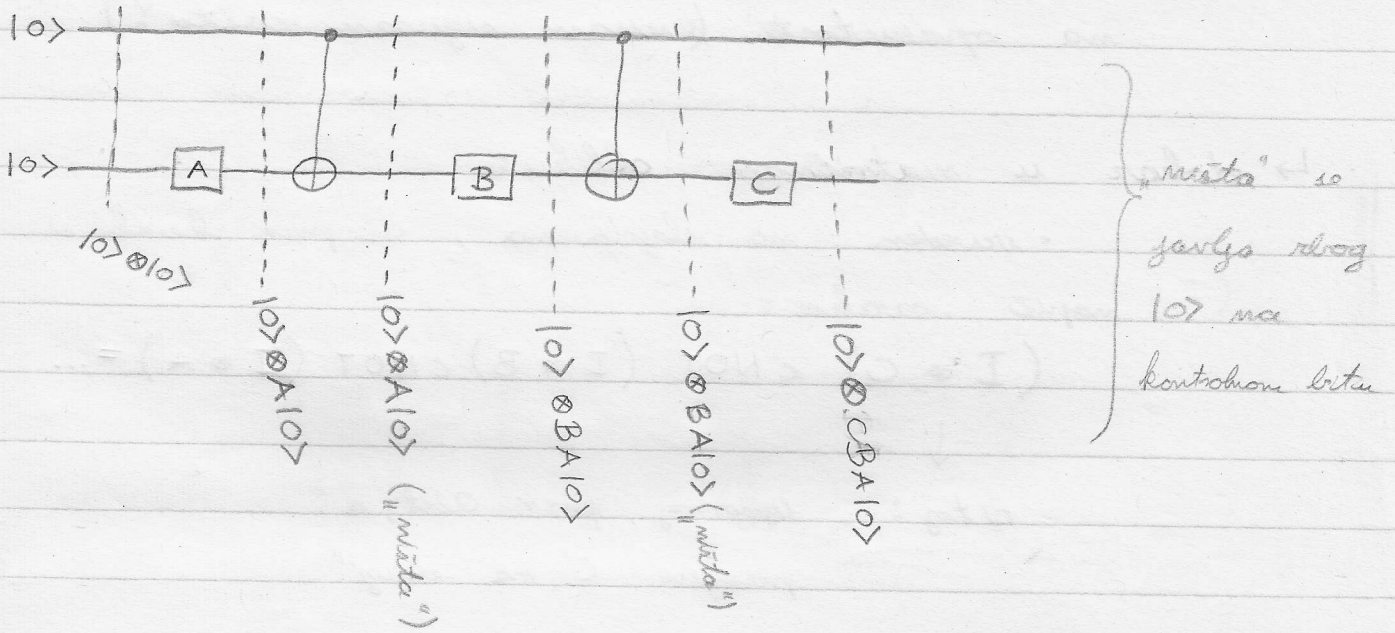
$$\begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$$

↳ primjeti da ako za operator U uzmemo σ_x, dobivamo cNOT vrata

PR: Operator cU možemo konstruirati pomoću cNOT vrata uz $CBA = I$ i $C\sigma_x B\sigma_x A = U$

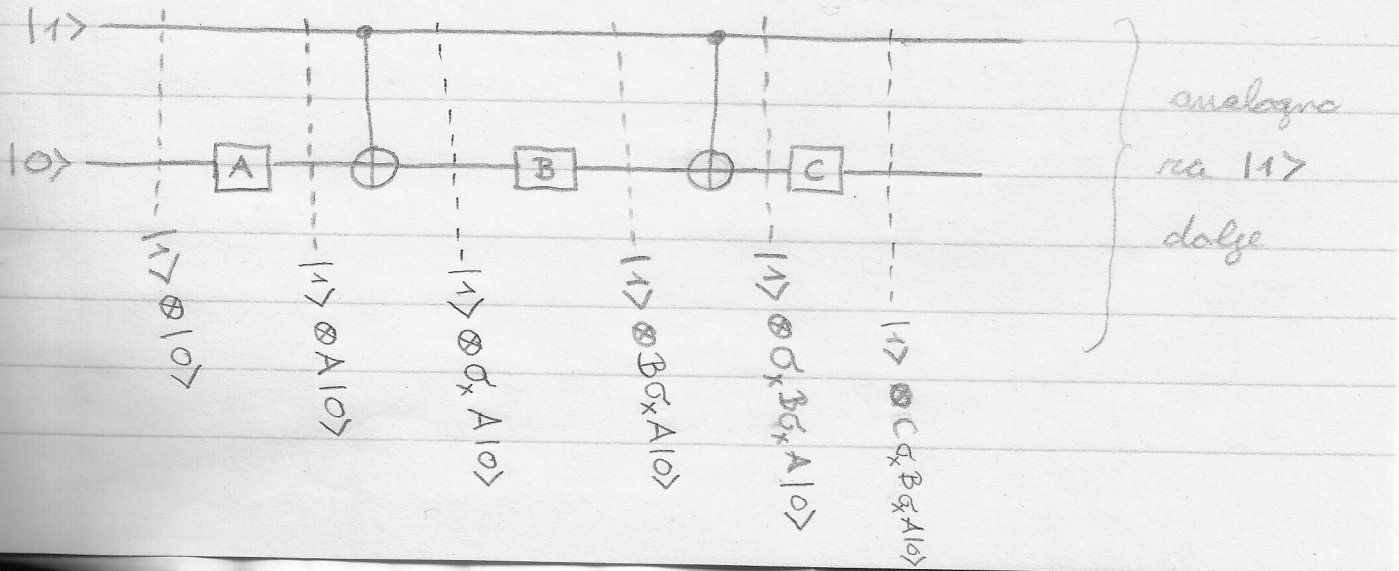


↳ provjerimo na način da pošaljemo $|0\rangle$ i gore i dolje, pa vidimo što se desi (ponovimo i za ostale ☺):



↳ za $|0\rangle$ i $|1\rangle$, sve je isto (samo je na žicama $|1\rangle$ umjesto $|0\rangle$)

↳ za $|1\rangle$ i $|0\rangle$ imamo:



↳ ovime smo isprobali sva bazna stanja kvantnog sustava da bi dokazali tvrdnju

↳ kontrolni bit i donji bit mogu biti bilo koja stanja $|\Phi\rangle$ i $|\Psi\rangle$, al nam je teško tako to provjeriti jer ionako moramo rastaviti na slučajeve

- ta stanja mogu biti spregnuta, pa ovime nismo prikazali svu ekspresivnost kvantnog sustava, al dokaz ne gubi na općenitosti (nisam siguran zašto!)

↳ dokaz u matričnom obliku:

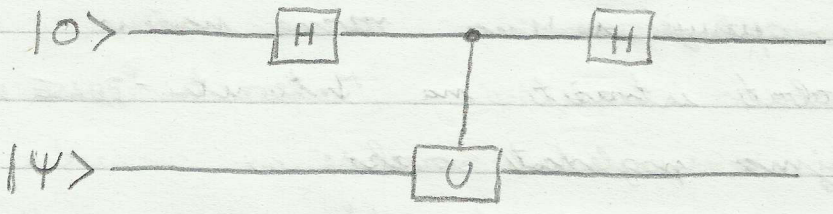
- izveden na slajdovima, a prvi korak si napiši ovako:

$$(I \otimes C)\ cNOT\ (I \otimes B)\ cNOT\ (I \otimes A) = \ldots$$

↓

čitaj: „ignoriraj prvi Qbit, a primjeni C na drugi"

PR: Pogledaj logički krug koji malo prikazuje snagu kvantnog računala zbog spregnutosti:



↳ inače, Hadamard „zbrčka" stanje, te ga ponovno vrati na stanje ako ponovno djeluje, no to u ovom primjeru nije tako!

• na gornjoj žici ne dobivamo |0> na kraju

↳ Hadamard služi da nemamo više sigurnost (kao u prethodnom primjeru) djelovanja CU vrata nego imamo bogatstvo kvantnog računala

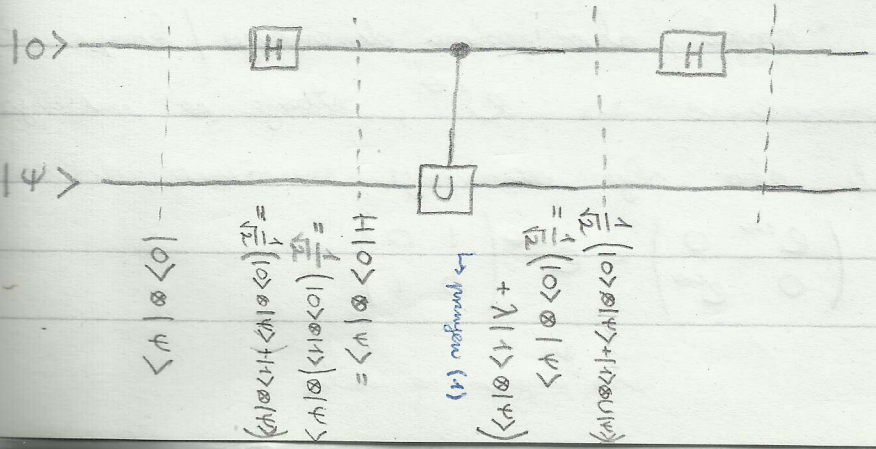
↳ trebamo sljedeće pretpostavke:

(1) $U|\phi\rangle = \lambda|\psi\rangle$; (2) $|\lambda| = 1$

↳ mora zbog unitarnost!

SHVATI KAKO PRIMJENITI SVOJSTVENU VRIJEDNOST!

↳ des se da je gornji prepleten, a donji neprepleten, pa provedimo ovo:



$\to \frac{1}{\sqrt{2}}\left(H|0\rangle\otimes|\psi\rangle + \lambda H|1\rangle\otimes|\psi\rangle\right)$

$= \frac{1}{\sqrt{2}}\left(H|0\rangle + \lambda H|1\rangle\right)\otimes|\psi\rangle$

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

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

⇒ kako to da je došla do promjene gornjeg bita, iako sma očekival i zbog cU vrata i zbog dva Hadamarda da neće doći do promjene?

↳ pa, opisuje se na razne načine (možeš probati istražit na Internetu - PHASE KISKBACK)

↳ pokušajmo pogledat ovako:

- pretpostavimo da U vrata ne djeluje na svoj (drugi) Qbit
- u stvari, pomnožio ga je sa nečim što ima modul jednak jedan i tako nije promjenio stanje:

a) $e^{i\phi} \cdot \begin{pmatrix} \mu \\ \nu \end{pmatrix} = e^{i\phi}$ } jedan Qbit

b) $e^{i\phi} \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$ } dva Qbita

⇓

nemoj to pomiješat sa operatorom rotacije $R[\theta]$:

- on mijenja stanje sustava

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix} = \begin{pmatrix} \mu \\ e^{i\theta}\nu \end{pmatrix}$$

- znači, ako jednu dimenziju / komponentu pomnožimo sa $e^{i\theta}$, stanje se mijenja, al ako obje dimenzije množimo, dobivamo:

$$\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix} = e^{i\theta} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

⇓

ne mijenja se ništa

⇒ no, pokušajmo odgovoriti na „phase kickback"
tako da se zapitamo što se des ako jedan
Qbit u sustavu dvaju Qbita pomnožimo sa
nečime modula 1:

↳ ništa se ne des i pokažimo to:

• konstruirajmo takav operator:

→ množenje jednog Qbita konstantom
u sustavu zapravo množi cijeli sustav
konstantom:

$$I \otimes \begin{pmatrix} \tilde{\sim} \\ \tilde{\sim} \\ \tilde{\sim} \end{pmatrix} = \begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{pmatrix} = \lambda I$$

⇒ UKRATKO:

uključiti $|\psi\rangle$

↳ ako je $|\psi\rangle$ mogući vektor, mogu separirat
stanja, pa možemo vidjet čudne pojave nazvane
„phase kickback"

↳ zbog separabilnost, uočavamo čudne pojave te
nam rezultat nisu očekivani

↳ množenje jednog Qbita u sustavu potpuno cijel sustav

KVANTNI ALGORITMI

⇒ KVANTNI PARALELIZAM:

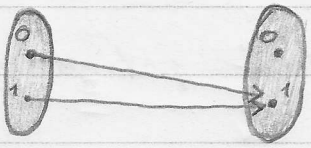
- radi se o tome da jednim prolaskom kroz kvantni krug, kvantno računalo dovlja račun sa svim kombinacijama barnih stanja
- pošto barna stanja odgovaraju bitarma klasičnog računala, kvantno računalo računa sve kombinacije ulaza klasičnog računala **odjednom**!

⇒ pogledajmo kako je David Deutch prezentirao kvantni paralelizam na „jednostavan" način:

↳ promotrimo sljedeću funkciju:

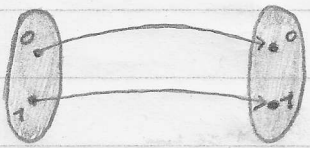
$$f: \{0,1\} \longrightarrow \{0,1\}$$

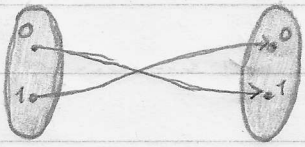




⇒ vrijedi: $f(0) = f(1)$

konstantne funkcije





⇒ vrijedi: $f(0) \neq f(1)$

uravnotežene funkcije

↳ Deutsch postavlja pitanje:

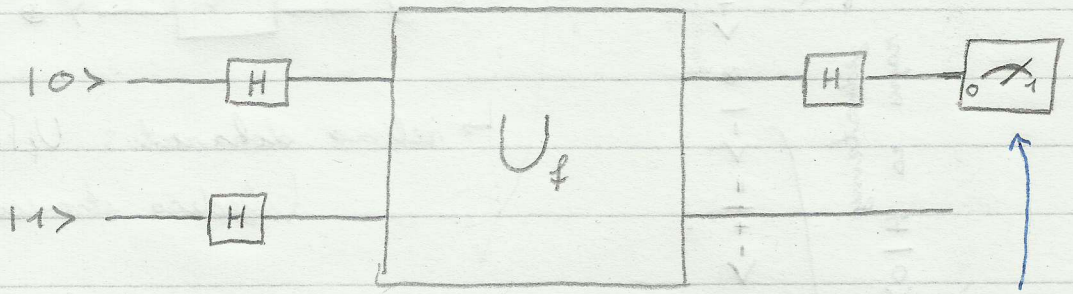
„Koliko puta moramo evaluirat funkciju „f" da saznamo je li ona konstantna ili uravnotežena?"

- na klasičnom računalu: 2 puta
- na kvantnom računalu pomoću Deutschovog algoritma: samo jednom

↳ na slajdu su prikazani klasična reverzibilna implementacija i kvantna implementacija

- razlika među njima je u tome da u kvantnu implementaciju možemo staviti neku superpoziciju stanja i evaluirat ju!

↳ Deutsch je je dodao još Hadamardova operatora kako bi dobio krug Deutschovog algoritma:



0 ⇒ konstantna

1 ⇒ uravnotežena

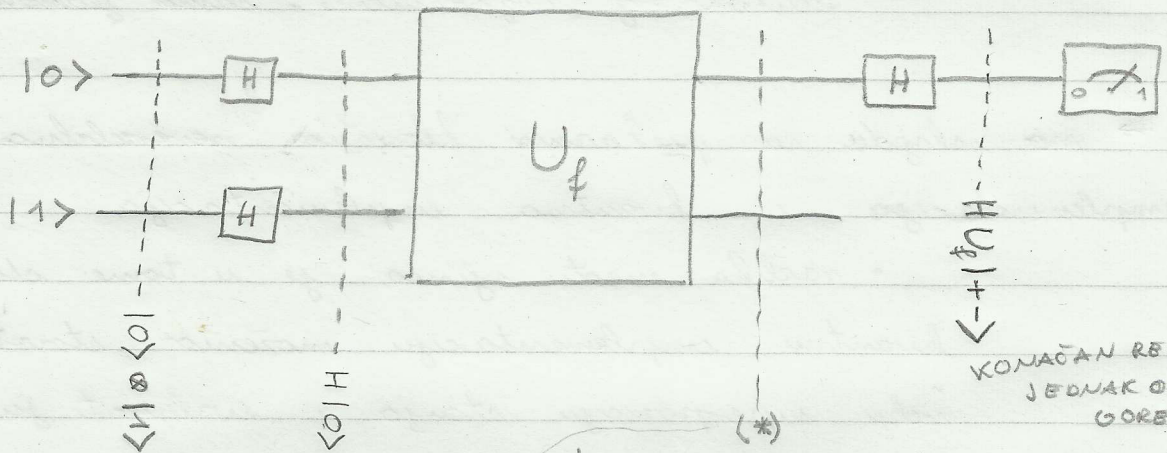
⇓

Deutsch je izračunao prirodnu funkciju ovog sustava i dobio odlučio konstantne il uravnotežene funkcije

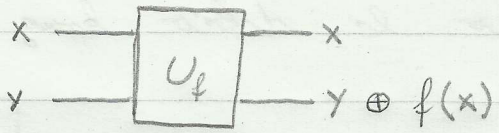
⇒ konačno stanje gornjeg Qubita je:

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

⇒ IZVOD DEUTSHOVOG ALGORITMA:



↳ ovdje je malo kompliciranije jer treba se vratit na funkciju U_f:



↳ želimo dokazat: $U_f|x-\rangle = (-1)^{f(x)}|x-\rangle$

(sljedeća stranica)

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

$$\Downarrow$$

separabilno stanje

(u zagradi je prvi bit)

(pretpostavi da je došlo do „phase kickback"-a)

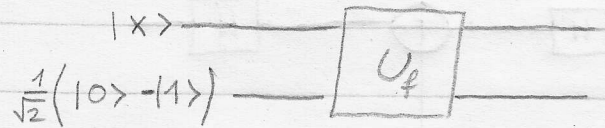
$$H|0\rangle \otimes H|1\rangle = |+\rangle \otimes |-\rangle = |+-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|-\rangle$$

samo jednostavniji zapis za $H|0\rangle$

samo jednostavniji zapis za $H|1\rangle$

⇒ pokažimo: $U_f |x-\rangle = (-1)^{f(x)} |x-\rangle$

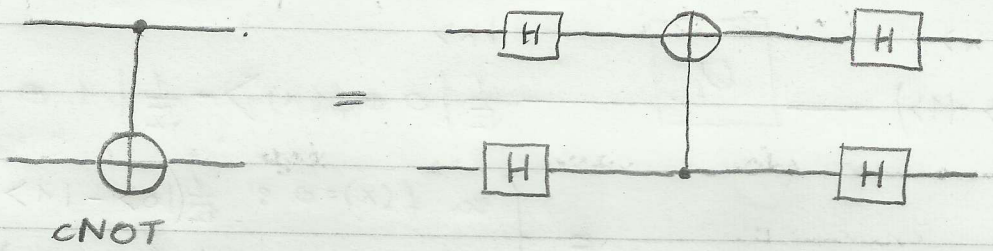
↳ prvo, pošaljimo unutra $|x\rangle$ i $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$:



$$= \begin{cases} \text{za } f(x)=0: \ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = +|-\rangle \\ \text{za } f(x)=1: \ \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = -|-\rangle \end{cases} =$$

$$= (-1)^{f(x)} |-\rangle$$

ZAD: Dokaži da je sljedeći operator (cNOT) ekvivalentan sljedećem logičkom krugu!



↳ primjena ovoga je borba protiv ograničenja u topologiji implementacije kvantnog čipa

- ako samo jedan qbit može biti kontrolni onom drugom, a obrat ne vrijedi tada možemo dobit obrat osim identitetom

⇒ prisjetimo se Hadamardovog operatora:

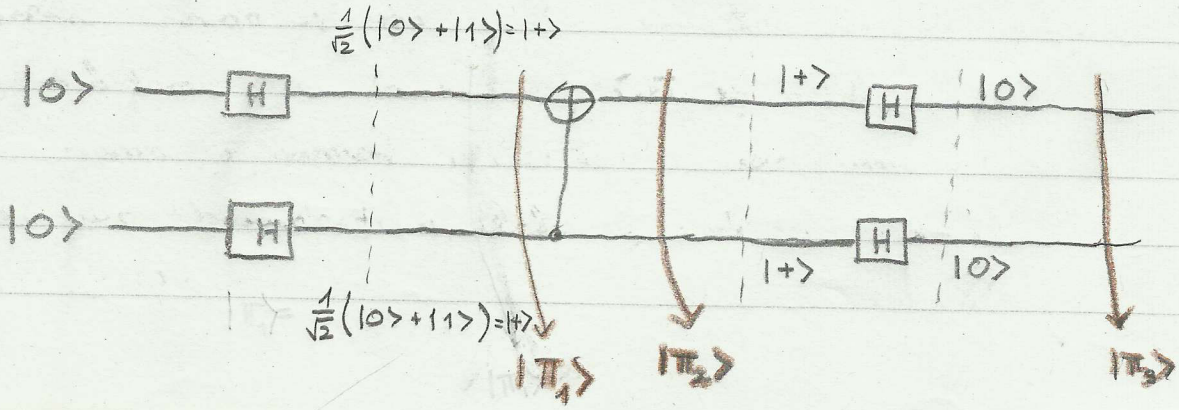
- on vrdjel stanje ravnomjerno na $|0\rangle$ i $|1\rangle$:

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

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

- možemo matrično, al to je kompliciranije jer trebamo tenzorski produkt dva Hadamarda što je matrica 4×4

⇒ pogledajmo ulaz $|0\rangle$ i $|0\rangle$



↳ raspišemo stanje $|\pi_1\rangle$ - tenzorski produkt $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$:

$$|\pi_1\rangle = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

↳ pišemo stanje sada $|\pi_2\rangle$ koje je nakon primjene cNOT operatora:

• NAPOMENA: bitno je kojeg člana pišemo prvog, a kojeg drugog kod cNOT operatora često da bi mogli biti usklađeni s matričnom notacijom sa slajdova

⇒ PRVI BIT JE LIJEVI (onaj na kojeg se djeluje), DRUGI BIT JE DESNI (kontrolni bit)

$$|\pi_2\rangle = \frac{1}{2}\left(|00\rangle + |11\rangle + |10\rangle + |01\rangle\right)$$

$$|\pi_2\rangle = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

↑

ostalo je isto samo rata jer je ispred svih $\frac{1}{2}$, pa su koeficijent ist (nije u općenitosti)

↳ pišemo krajnje stanje $|\pi_3\rangle$ koje je ravnino stanje:

• kako je $|\pi_1\rangle = |\pi_2\rangle$ i ovo je separabilno jer je to tenzorski $|+\rangle \otimes |+\rangle$, Hadamard djeluje na svakog posebno, a kako je Hadamard sam sebi inverz, vrijedi $H|+\rangle \otimes H|+\rangle = |0\rangle \otimes |0\rangle = |\pi_3\rangle$

↳ no, kako bi dobil $|\pi_3\rangle$ da nismo uspjeli raklopiti da je stanje separabilno (i da nismo uspjeli prepoznat da je ovo $|+\rangle \otimes |+\rangle$)

• eh, onda moraš napisati preko matrice i množiti matrice što se ne preporuča

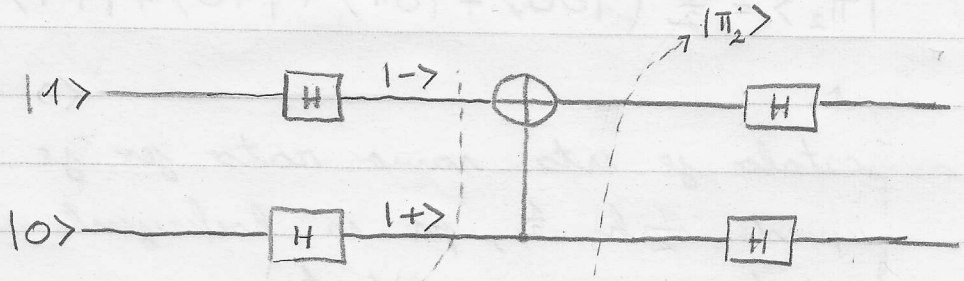
⇒ <u>sada, ovo ponavljamo za ulaze:</u>

a) $|01\rangle$

↳ vrlo slično jer je kontrolni bit opet u nulu, pa se bit na koj se djeluje ne mijenja

b) $|10\rangle$

↳ ovo ćemo sada provesti nešto brže



$$|\pi_1\rangle = |-+\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

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

$$|\pi_2\rangle = \frac{1}{2}(|00\rangle + |11\rangle - |10\rangle - |01\rangle)$$

↳ $|\pi_2\rangle$ treba zapisati kao tenzorski kako bi mogli primjeniti Hadamarda na svaku komponentu

↳ pokazuje se da je: $|\pi_2\rangle = |-\rangle \otimes |-\rangle$

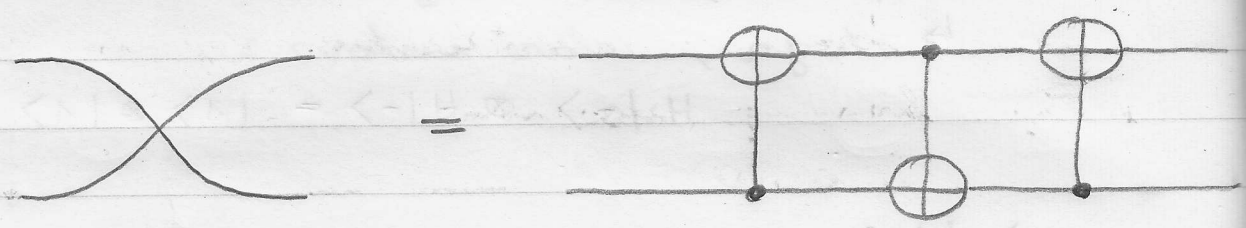
↳ stoga, izlaz sustava:

$$H|-\rangle \otimes H|-\rangle = |1\rangle \otimes |1\rangle$$

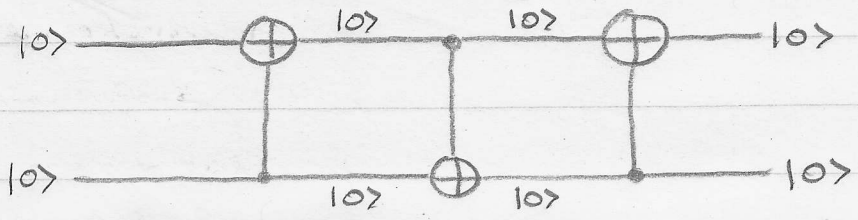
c) $|11\rangle$

↳ analogno prethodnim primjerima, pa ga nećemo posebno razmatrati!

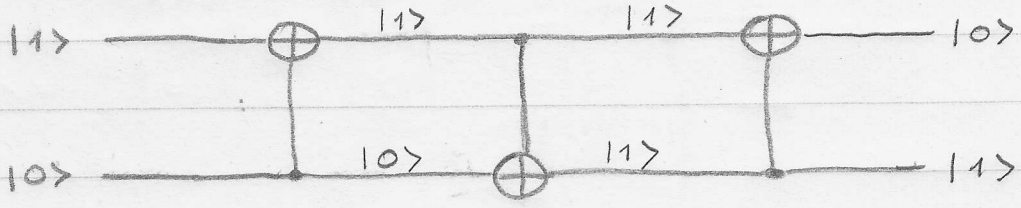
ZAD: Primjet i za vježbu dokaži da je zamjena žica ekvivalentna „pametnoj" primjeni cNOT operatora:



↳ uzmimo na ulaz $|00\rangle$:



↳ uzmimo na ulaz $|10\rangle$:



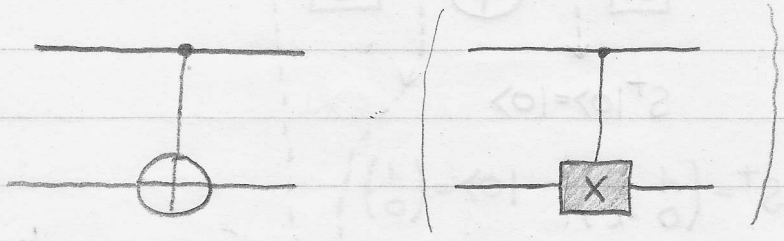
↳ za $|01\rangle$ i $|11\rangle$ je analogno, pa nećemo posebno dokazivat

↳ ovo je bilo laganije jer nije bilo Hadamarda koj bi prijetio neseparabilnošću nego smo bil siguru da sve ostaje separabilno

GROVEROV ALGORITAM

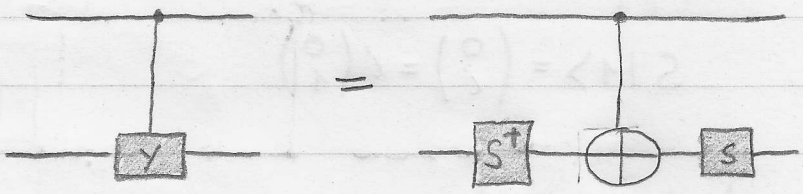
⇒ prije uvođenja novog algoritma, valja se podsjetiti s nekim logičkim identitetima koj nam služe za izgradnju kvantnog algoritma:

a) c-NOT:
(control X)

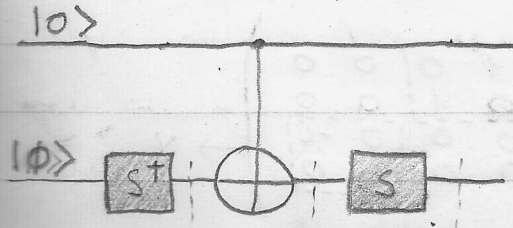


↳ druga oznaka jer je cNOT u matričnom obliku σ_x što znači stanje oko x-osi za kut π
(analogno rotacija za σ_x i σ_y)

b) operator σ_y:
(control Y)



↳ dokažimo da gore pustimo $|0\rangle$, a dolje neko stanje $|\phi\rangle$:

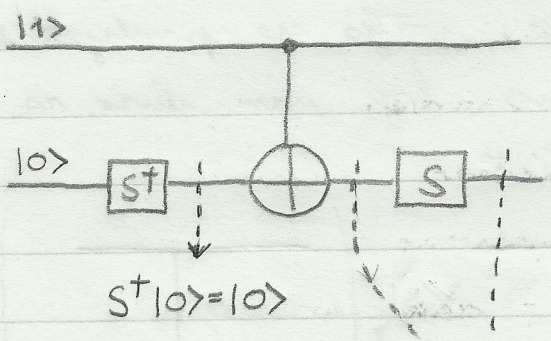


$S^\dagger|\phi\rangle$ $S^\dagger|\phi\rangle$ $SS^\dagger|\phi\rangle = |\phi\rangle$

unitarno, pa je 1

} ovo je lako slučaj jer je gore $|0\rangle$, pa cNOT ne djeluje

↳ sada gore pustimo $|1\rangle$ i pogledajmo dva slučaja - dolje je $|0\rangle$ i zatim $|1\rangle$:



$$S^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} \quad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$S^\dagger|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$S|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

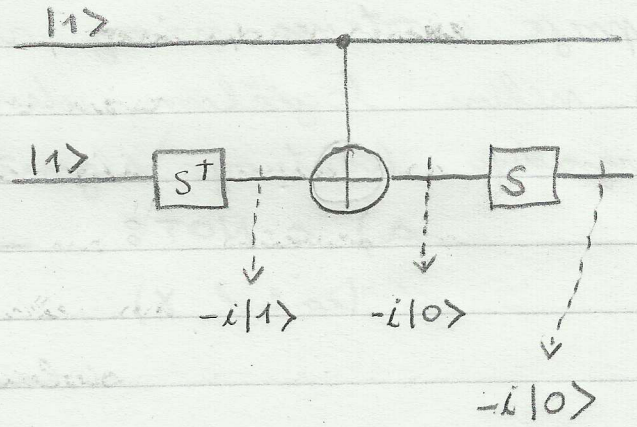
$$S|1\rangle = \begin{pmatrix} 0 \\ i \end{pmatrix} = i \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

↳ znači, ako smo pustili $|10\rangle$ dobivamo $i|11\rangle$:

$$\boxed{|10\rangle \rightarrow i|11\rangle}$$

↳ provjera matrično:

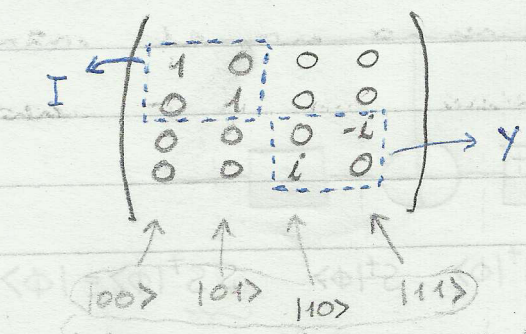
$$|11\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} (0\ 1)$$



ovo možemo tako brzo jer smo vidjeli prošli slučaj što $S^\dagger$ i S rade ($S^\dagger$ množi drugi sa „$-i$", a S sa „i")

$$\boxed{|11\rangle \rightarrow -i|10\rangle}$$

↳ iz dobivenog možemo napisati matricu ovog operatora (kombinacija ulaza su po stupcima):



ulazi, a izlazi su po stupcima

⇒ NAPOMENA: svaki ciklus na kvantnom računalu (ciklus gledamo kao prolaz kroz kvantna vrata) povećava **dekoherenciju** i to **eksponencijalno**, stoga:

- težimo što manjem broju vrata, pa želimo algoritme dobro optimizirati pametnim slaganjem operatora
- prisjetimo se - dekoherencija smanjuje sigurnost u dobiveno rješenje jer Qbitovi gube stabilnost //

c) operator σ_z:
(control Z)

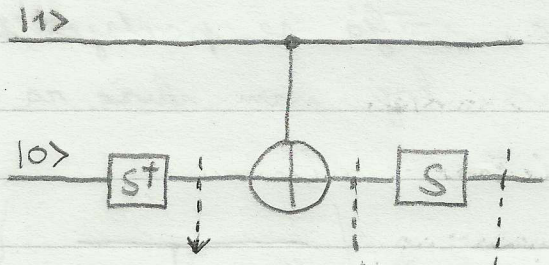


↳ ovo si dokaži sam ∇.

↳ nije potrebno pisat $H^\dagger$ jer je Hadamardov operator sam sebi inverz, al se ovo piše iz pristojnost da se zna na što se misli

⇒ sada imamo sve što nam treba da bi riješili i pokazali Groverov algoritam ∇.

↳ sada gore pustimo $|1\rangle$ i pogledajmo dva slučaja - dolje je $|0\rangle$ i zatim $|1\rangle$:



$S^\dagger|0\rangle = |0\rangle$

$S^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} \quad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$S^\dagger|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$

$|1\rangle$

$S|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

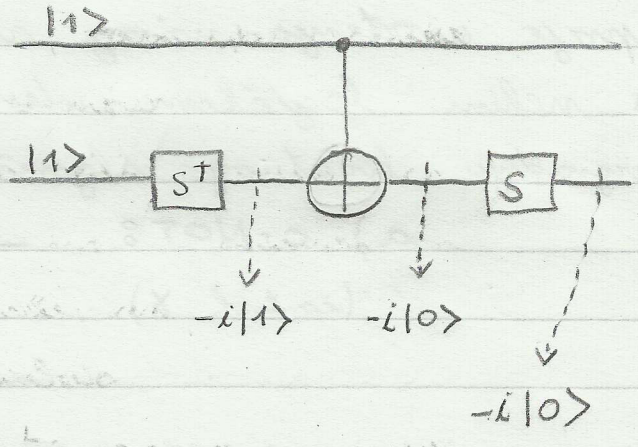
$S|1\rangle = \begin{pmatrix} 0 \\ i \end{pmatrix} = i\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

↳ znači, ako smo pustil $|10\rangle$ dobivamo $i|11\rangle$:

$$\boxed{|10\rangle \rightarrow i|11\rangle}$$

↳ provjera matrično:

$|11\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}(0\ 1)$



ovo možemo tako brzo jer smo vidjel prošl slučaj što $S^\dagger$ i S rade ($S^\dagger$ množ drug sa „$-i$", a S sa „i")

$$\boxed{|11\rangle \longrightarrow -i|10\rangle}$$

↳ iz dobivenog možemo zapsat matricu ovog operatora (kombinacija ulaza su po stupcima):

$$\begin{array}{c} \\ I \leftarrow \\ \\ \\ \end{array}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{pmatrix} \rightarrow Y$$

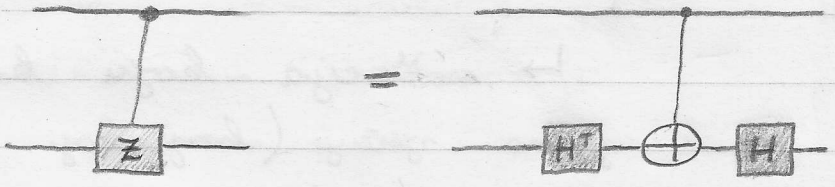
$|00\rangle \quad |01\rangle \quad |10\rangle \quad |11\rangle$

ulazi, a izlazi su po stupcima

⇒ NAPOMENA: svaki ciklus na kvantnom računalu (ciklus gledamo kao prolaz kroz kvantna vrata) povećava **dekoherenciju i to eksponencijalno**, stoga:

- težimo što manjem broju vrata, pa želimo algoritme dobro optimizirati pametnim slaganjem operatora
- prisjetimo se - dekoherencija smanjuje sigurnost u dobiveno rješenje jer Qbitovi gube stabilnost //

c) operator σ_z:
(control Z)

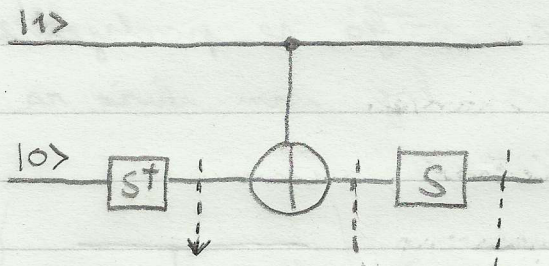


↳ ovo si dobari sam ▽.

↳ nije potrebno pisat $H^\dagger$ jer je Hadamardov operator sam sebi inverz, al se ovo piše iz pristojnosti da se zna na što se misli.

⇒ sada imamo sve što nam treba da bi riješili i pokarali Groverov algoritam ▽.

↳ sada gore pustimo $|1\rangle$ i pogledajmo dva slučaja - dolje je $|0\rangle$ i zatim $|1\rangle$:



$S^\dagger|0\rangle = |0\rangle$

$S^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$ $\quad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$S^\dagger|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$

$|1\rangle$

$S|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

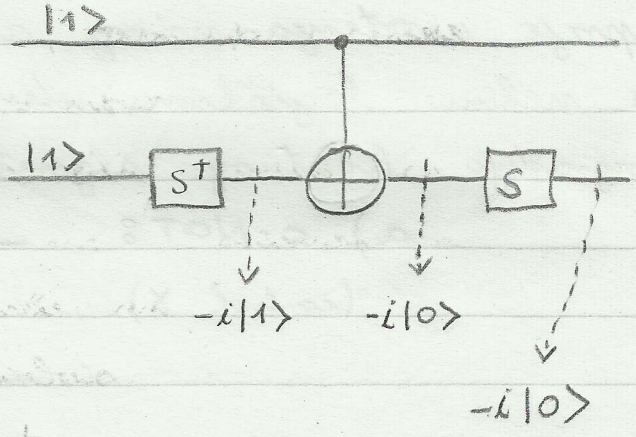
$S|1\rangle = \begin{pmatrix} 0 \\ i \end{pmatrix} = i\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

↳ znači, ako smo pustil $|10\rangle$ dobivamo $i|11\rangle$:

$$\boxed{|10\rangle \rightarrow i|11\rangle}$$

↳ provjera matrično:

$|11\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}(0\ 1)$



ovo možemo tako brzo jer smo vidjel prošl slučaj što $S^\dagger$ i S rade ($S^\dagger$ množ drug sa „$-i$", a S sa „i")

$$\boxed{|11\rangle \longrightarrow -i|10\rangle}$$

↳ iz dobivenog možemo zapsat matricu ovog operatora (kombinacije ulaza su po stupcima):

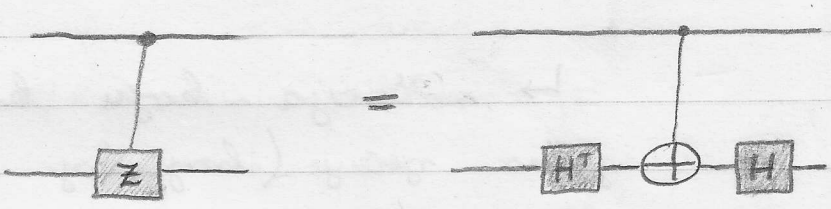
$$\begin{array}{cc} & \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{array}{c} I \leftarrow \\ \\ \\ \\ \end{array} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{pmatrix} \begin{array}{c} \\ \\ \rightarrow Y \\ \\ \end{array} \end{array}$$

ulazi, a izlazi su po stupcima

⇒ NAPOMENA: svaki ciklus na kvantnom računalu (ciklus gledamo kao prolaz kroz kvantna vrata) povećava **dekoherenciju i to eksponencijalno**, stoga:

- težimo što manjem broju vrata, pa želimo algoritme dobro optimizirati pametnim slaganjem operatora
- prisjetimo se - dekoherencija smanjuje sigurnost u dobiveno rješenje jer Qbitovi gube stabilnost //

c) operator σ_z: (control Z)



↳ ovo si dokaži sam ∇

↳ nije potrebno pisat $H^\dagger$ jer je Hadamardov operator sam sebi inverz, al se ovo piše iz pristojnost da se zna na što se misli

⇒ sada imamo sve što nam treba da bi rješili, pokaral Groverov algoritam ∇

⇒ GROVEROV ALGORITAM

↳ rješava problem pretrage nestrukturirane baze podataka

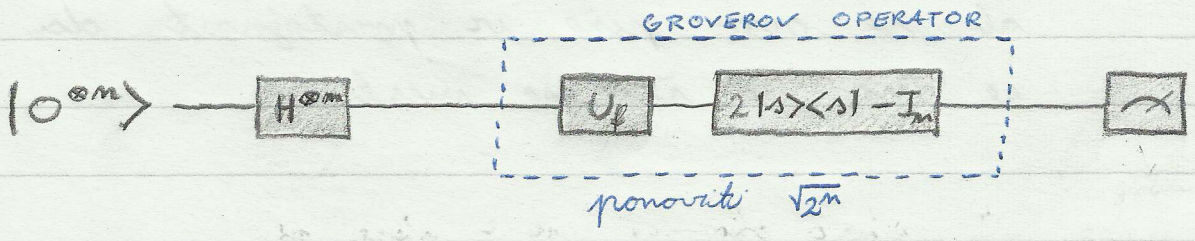
- npr. ako telefonski imenik pretražujemo po broju (a ne po imenu), to je nestrukturirana baza podataka i u prosjeku nam na klasičnom računalu prolaženo pola imenika da nađemo broj koji želimo

↳ Grover vel da u ovo na kvantnom računalu može puno bolje!

↳ notacija koju koristimo nalaže da imamo jedno rješenje (broj koji tražimo) u ukupno 2^n zapisa („n" - qubita sustav):

$x = 0, \dots, 2^n - 1$ (stoga, na klasičnom radimo $\frac{2^n}{2}$)

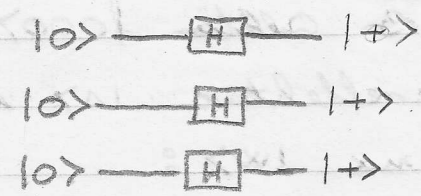
↳ logički krug Groverovog algoritma:



↳ znači, ovaj algoritam garantira da rješenje nalazimo u $\sqrt{2^n}$ koraka što je puno puno bolje od „u prosjeku" $\frac{2^n}{2}$ puta!

↳ napravimo analizu Groverovog algoritma za primjer od 3 Qubita (pretraživanje 3 stanja):

1) sve Qbitove propuštamo kroz Hadamard



$$|+\rangle \otimes |+\rangle \otimes |+\rangle =$$

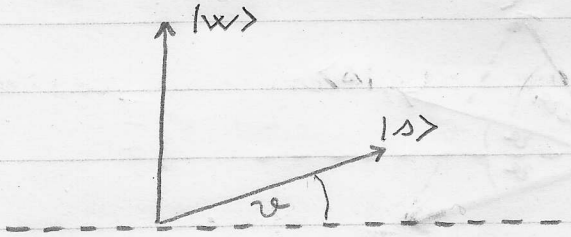
$$= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$= \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + \ldots + |111\rangle)$$

$$= |s\rangle$$

↖ stanje „s" za „superpozicija"

↳ primjećujemo da za velik „n", stanje $|s\rangle$ je „skoro okomito" na traženo stanje $|w\rangle$ jer je $|w\rangle$ jedan od stanja $|000\rangle$, $|001\rangle$, ..., $|111\rangle$ (za velik „n" ih je više), a svi ti vektori stanja sudjeluju malo u toj superpoziciji (i to jednako).

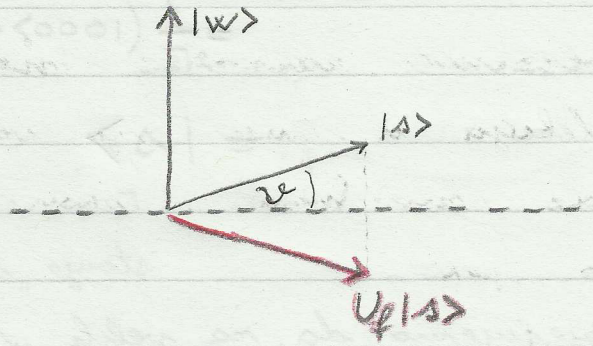


↳ „skoro okomito" nam dođe da radimo aproksimaciju:

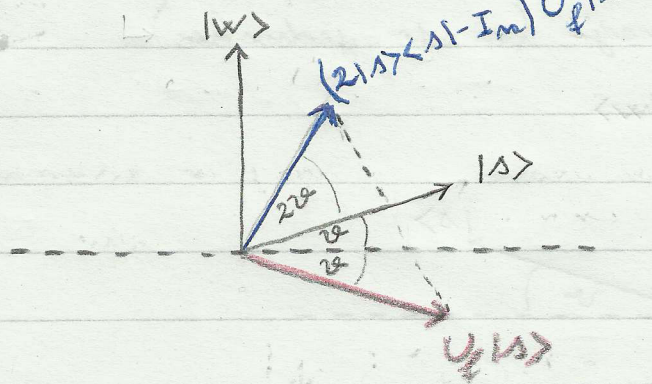
$$\theta \approx \sin\theta = \langle w|s\rangle = \frac{1}{\sqrt{2^n}}.$$

2) operator U_f na početni vektor stanja rad to da promjeni predznak uz baru vektor $|w\rangle$ (sjeti se, $|w\rangle$ je jedan od vektora računalne baze što je za 3 qbita $|000\rangle, |001\rangle, \ldots, |111\rangle$)

↳ to zapravo reflektira $|s\rangle$ u odnosu na hiperravninu okomitu na $|w\rangle$:



3) operator $2|s\rangle\langle s| - I_m$ možemo shvatit kao refleksiju u odnosu na vektor $|s\rangle$ (dokazat ćemo da je to tako)



↳ vidimo da je $(2|s\rangle\langle s| - I_m)U_f|s\rangle$ bliže rješenju $|w\rangle$ nego početno $|s\rangle$ jer smo dival samo onu dimenziju u kojoj s $|s\rangle$ i $|w\rangle$

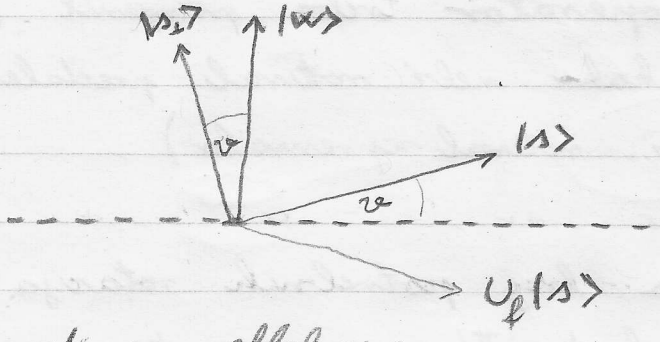
↳ time smo povećali vjerojatnost mjerenja traženog rješenja te se taj trik zove AMPLITUDE AMPLIFICATION

4) Groverov algoritam vel. da koraka 2) i 3) ponavljamo $\sqrt{2^n}$ puta kako bi se pomaknuli gotovo točno na $|w\rangle$

5) obavljamo mjerenje i dekodiramo rješenje

⇒ pokušajmo sada dizajnirati što je operator $2|s\rangle\langle s| - I_n$ refleksija u odnosu na vektor $|s\rangle$:

• znamo da postoj (negdje) okomica $|s_\perp\rangle$



• gradimo refleksiju:

$$I_n - |s_\perp\rangle\langle s_\perp| + (-1)|s_\perp\rangle\langle s_\perp| = (*)$$

skidamo komponentu u ravnini — dodajemo komponentu u ravnini

$$(*) = I_n - 2|s_\perp\rangle\langle s_\perp| =$$

↕ ovo je malo teže skužit

$$= |s\rangle\langle s| + |s_\perp\rangle\langle s_\perp| - 2|s_\perp\rangle\langle s_\perp| =$$

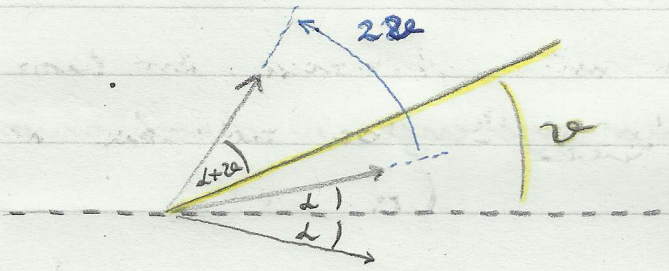
$$= 2|s\rangle\langle s| - |s\rangle\langle s| - |s_\perp\rangle\langle s_\perp| =$$

↑ ista ova fora kao i gore

$$= 2|s\rangle\langle s| - I_n$$

DOBILI SMO OPERATOR REFLEKSIJE!

⇒ važno je sjetiti se da su dvije refleksije uvijek rotacija (to znamo iz linearne algebre):



↳ stoga, Groverov operator možemo shvatiti kao rotaciju za kut 2θ prema rješenju $|w\rangle$

↳ to nam je potrebno kako bi dobavili da Groverov operator treba primijeniti „oko" $\sqrt{2^n}$ puta (ne više kako nebi rotirali predaleko, ne manje kako nebi rotirali premalo)

⇒ odredimo sada broj potrebnih rotacija da bi se zarotirali za kut $\pi/2$ jer je tamo rješenje $|w\rangle$:

$$\theta + k(2\theta) = \frac{\pi}{2}$$

$$\theta(2k+1) = \frac{\pi}{2} \Rightarrow 2k+1 = \frac{\pi}{2}\cdot\frac{1}{\theta}$$

$$2k+1 = \frac{\pi}{2}\cdot\sqrt{2^n}$$

$$\boxed{k = \frac{1}{2}\left(-1+\frac{\pi}{2}\sqrt{2^n}\right)}$$

⇒ ovo je strihtno, ali je Grover ovo aproksimirao sa:

$$k = \sqrt{2^n}$$

KVANTNA TELEPORTACIJA

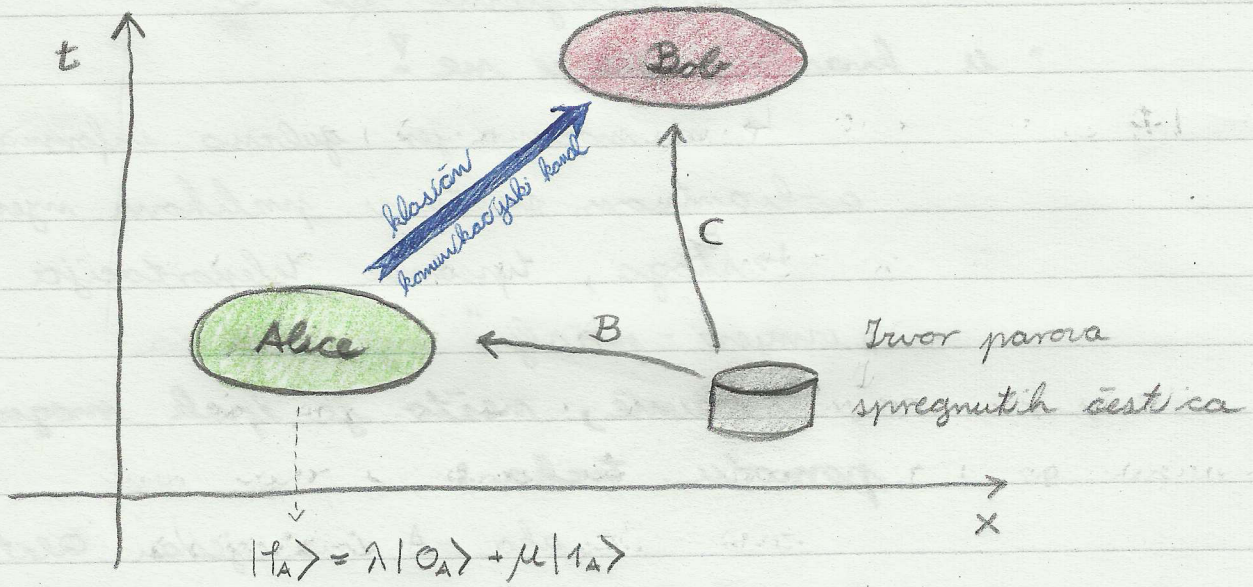
⇒ je li moguće prenijeti informaciju kvantnog sustava od točke A do točke B bez gubitka informacije

- u klasičnog fizici da!
  - ↳ izmjeri veličinu i pošalji pismo s informacijama do B
- u kvantnoj fizici ne!
  - ↳ ne možemo jer gubimo informaciju o kvantnom sustavu prilikom mjerenja
  - ↳ stoga, tipična teleportacija „izmjeri - pošalji" nije moguća
  - ↳ **naime, nešto je ipak moguće pomoću trika:**
    - ako A ima jedan Qbit i B ima jedan Qbit koji su spregnuti, na mjestu A možemo izmjeriti Qbit (uništiti ga) i poslati informaciju na točku B
    - tada se na točki B može rekonstruirati stanje Qbita A

TO JE KVANTNA TELEPORTACIJA

⇒ o ovome možemo razmišljati kao da je laboratorij u kojem su Qbit A i Qbit B na dva mjesta odjednom

⇒ NAPOMENA: primjeti da prilikom ovog postupka nije narušen teorem o nemogućnosti kvantnog kloniranja jer se prilikom mjerenja na mjestu A uništava taj Qbit i onda se rekonstruira na B (nije moguće da ga A pošalje na B, a da on ostane i na A)



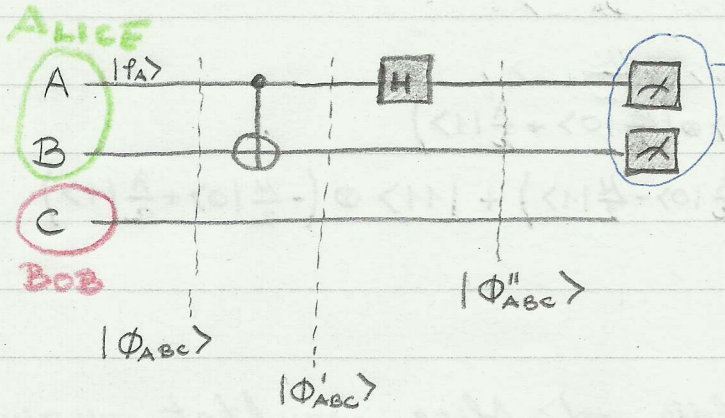
↳ u prijašnjem tekstu su A i B bila mjesta laboratorija, a na crteži su to Alice i Bob (onake B i C su onake dva Qbita)

↳ početno stanje para BC:

$$|\psi_{BC}\rangle = \frac{1}{\sqrt{2}}\left(|0_B 0_C\rangle + |1_B 1_C\rangle\right)$$

(pretpostavljeno da je stanje spregnuto)

⇒ nacrtajmo kvantno logički krug ovog eksperimenta:



$$|\Phi_{ABC}\rangle = |\psi_A\rangle \otimes \frac{1}{\sqrt{2}}\left(|0_B 0_C\rangle + |1_B 1_C\rangle\right) =$$

$$= \frac{\lambda}{\sqrt{2}}|0_A\rangle \otimes \left(|0_B 0_C\rangle + |1_B 1_C\rangle\right) + \frac{\mu}{\sqrt{2}}|1_A\rangle \otimes \left(|0_B 0_C\rangle + |1_B 1_C\rangle\right)$$

↳ to je na početku - tada Alice to provuče kroz cNOT i Hadamardova vrata da stvori jednostavnu interakciju (nemoj se zamarati zašto baš ovi operatori):

$$|\Phi'_{ABC}\rangle = \frac{\lambda}{\sqrt{2}}|0_A\rangle \otimes \left(|0_B 0_C\rangle + |1_B 1_C\rangle\right) + \frac{\mu}{\sqrt{2}}|1_A\rangle \otimes \left(|1_B 0_C\rangle + |0_B 1_C\rangle\right)$$

$$|\Phi''_{ABC}\rangle = H|\Phi''_{ABC}\rangle = \frac{\lambda}{2}\left(|0_A\rangle + |1_A\rangle\right)\otimes\left(|0_B 0_C\rangle + |1_B 1_C\rangle\right)$$

$$+ \frac{\mu}{2}\left(|0_A\rangle - |1_A\rangle\right) \otimes \left(|1_B 0_C\rangle + |0_B 1_C\rangle\right) =$$

$$= \frac{\lambda}{2}|000\rangle + \frac{\lambda}{2}|011\rangle + \frac{\lambda}{2}|100\rangle + \frac{\lambda}{2}|111\rangle + \frac{\mu}{2}|010\rangle + \frac{\mu}{2}|001\rangle - \frac{\mu}{2}|110\rangle - \frac{\mu}{2}|101\rangle$$

↳ sada ćemo prolat stanje razdvojiti tako da pogledamo sva 4 slučaja koje Alice može izmjeriti

↳ samo lepše napišemo $|\Phi''_{ABC}\rangle$ po mogućim mjerenjima za Alice:

$$|\Phi''_{ABC}\rangle = |00\rangle \otimes \left(\frac{\lambda}{2}|0\rangle + \frac{\mu}{2}|1\rangle\right) + |01\rangle \otimes \left(\frac{\mu}{2}|0\rangle + \frac{\lambda}{2}|1\rangle\right)$$
$$+ |10\rangle \otimes \left(\frac{\lambda}{2}|0\rangle - \frac{\mu}{2}|1\rangle\right) + |11\rangle \otimes \left(-\frac{\mu}{2}|0\rangle + \frac{\lambda}{2}|1\rangle\right)$$

↳ to je to!

- ako Bob dobije od Alice rezultat njezinog mjerenja, i recimo dobije $|00\rangle$, tada Bob može reći da je njegov Qbit u stanju $\frac{\lambda}{2}|0\rangle + \frac{\mu}{2}|1\rangle$
- da Alice mjeri $|01\rangle$, tada Bob mora svoj Qbit C propustiti kroz NOT da bi bio siguran da je njegov Qbit u stanju kao i Alicov Qbit ($|01\rangle$)
- da Alice mjeri $|10\rangle$ Bob mora propustiti svoj Qbit C kroz σ_z („phase-shift") da dobije isto stanje koje je imala Alice
- da Alice mjeri $|11\rangle$ Bob mora propustiti svoj Qbit C kroz σ_z i zatim kroz NOT i onda ima isto stanje kao i Alice ($|11\rangle$)