Erwin Schrödinger

Uvod v kvantno mehaniko

Trend miniaturizacije

- **Svet tranzistorjev**
  - Velikost tranzistorjev se zmanjšuje (Moorov zakon)
  - Posamezen tranzistor je tako majhen, da je bližje svetu kvantne mehanike kot pa svetu klasične mehanike
  - Vendar pa se informacija, ki jo oblikujejo ti tranzistorji še vedno interpretira na klasičen način.
  - Zato tvorijo takšni tranzistorji klasična vrata in posledično klasičen računalnik.

- **Kvantni nivo daje računalnikom dostop do novih fizikalnih učinkov**
  - Superpozicija, Interferenca, Kvantno prepletanje (entangulacija), nelokalnost, nedeterminističnost, neizvedljivost kloniranja
  - novi pristopi k algoritmom

- **Nanotehnologija "per se" ne izkorišča vseh kvantnih pojavov**
  - Da bi povečali učinkovitost računalnikov, je potrebno izkoristiti edinstvenost vseh kvantnih učinkov, npr. tudi kvantnega prepletanja (entangulacije)

Atomi in praznina

- *“Po dogovoru obstaja sladkost. Po dogovoru obstaja grenkoba. Po dogovoru obstaja barva. V resnici obstajajo le atomi in praznina."* Demokrit, 450 pr. n. št., Abdera
- razprava še vedno poteka med atomisti in anti-atomisti: vprašanje v tej razpravi je, ali sta prostor in čas sestavljena iz nedeljivih delcev, na Planckovi ločljivosti 10^{-33} centimetrov oz. 10^{-43} sekunde.

Quantum Computing Since Democritus
(http://scottaaronson.com/democritus/default.html)

Schrödingerjeva enačba

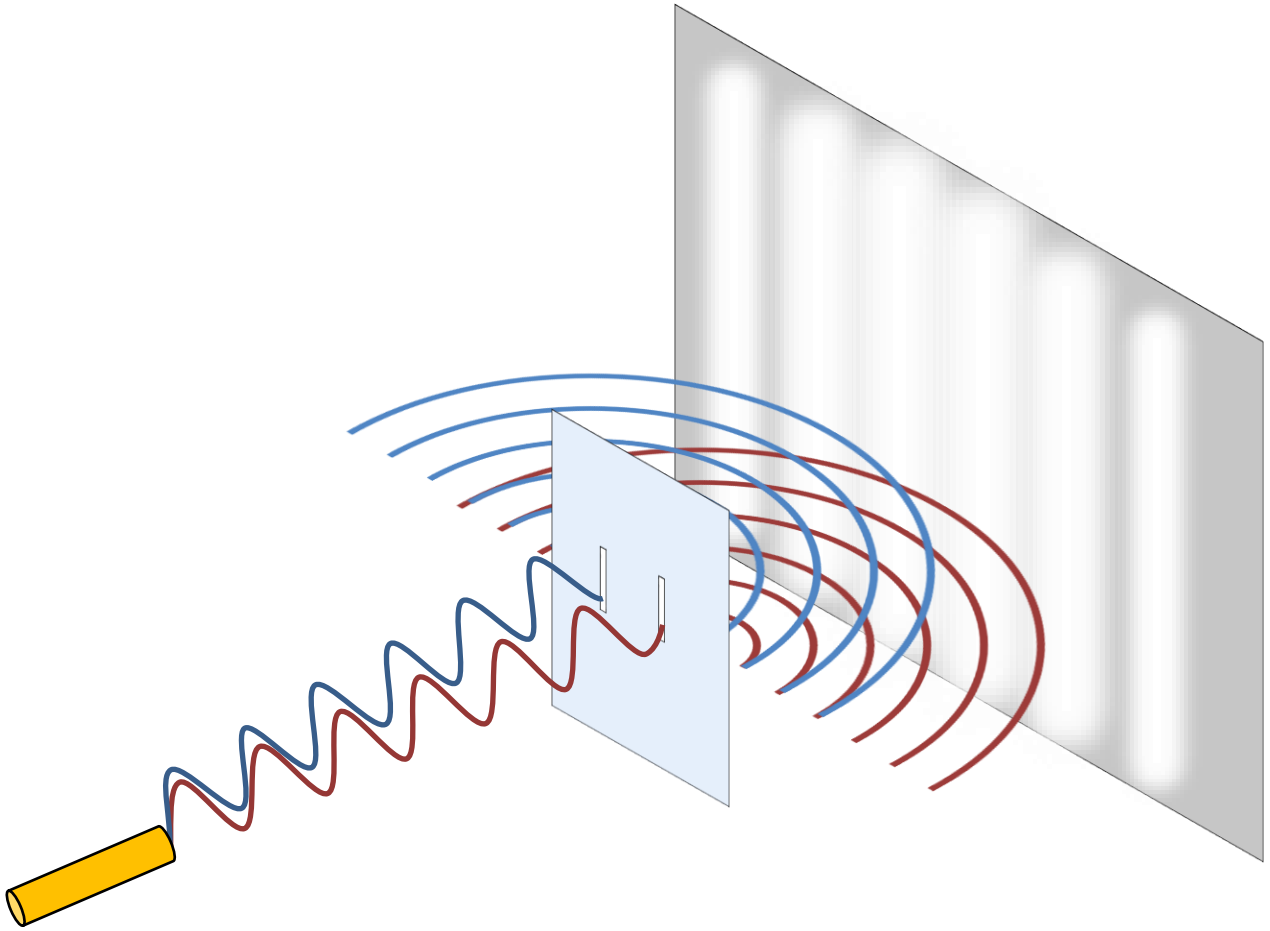
$$i\hbar\frac{\partial}{\partial t}\Psi(\mathbf{r},t)=\hat{H}\Psi(\mathbf{r},t)$$

- kjer je
  - i imaginarna enota ($i^2=-1$)
  - $\hbar$ Planckova konstanata (6.582×10^{-16} eV·s)
  - $\Psi(\mathbf{r},t)$ valovna funkcija; verjetnostna amplituda različnih konfiguracij opazovanega sistema v času t in poziciji $\mathbf{r}$
  - $\hat{H}$ Hamiltonov operator

- Za vsako izolirano regijo v vesolju, ki jo želite obravnavati, opisuje ta enačba razvoj stanja te regije v času. Stanje opišemo kot normalizirano linearno kombinacijo - superpozicijo - vseh možnih konfiguracij osnovnih delcev v tej regiji.

Double Slit Experiment

Eksperiment z dvojno režo

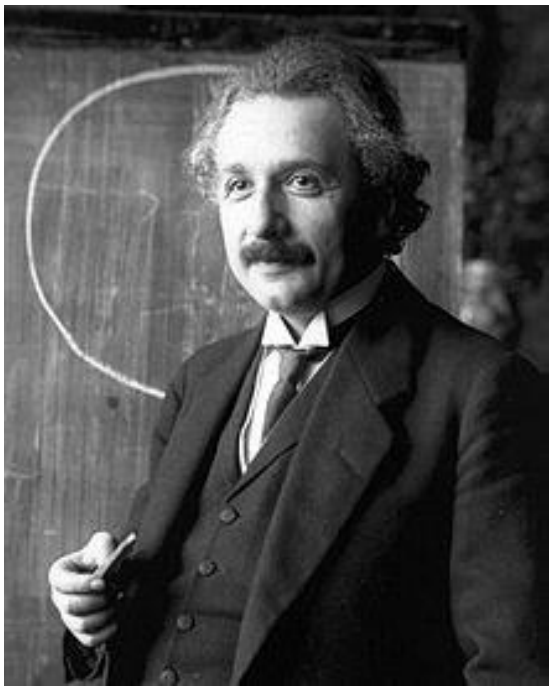


Dr Quantum - Double Slit Experiment
(youtube)

https://www.youtube.com/watch?v=Q1YqgPAtzho

Človeški opazovalec in superpozicija

- **Kopenhagenska (epistemološka) interpretacija**
  - Kvantna mehanika opisuje **izide naših meritev in naše dojemanje** in ne podaja nujno objektiven opis oz. resnično stanje kvantnega sistema. Je le teorija o našem znanju. (Niels Bohr)
- **Interpretacija več svetov**
  - Ob vsakem dogodku z več možnimi izidi se **vesolje razcepi**.
- **Kvantna informacija**
  - **Merjen sistem in merilni sistem se med meritvijo neločljivo prepleteta**. Dobimo novo prepleteno stanje (kvantni preplet ali entangulacija), v katerem merjenega in merilnega sistema ne moremo več informacijsko ločiti.

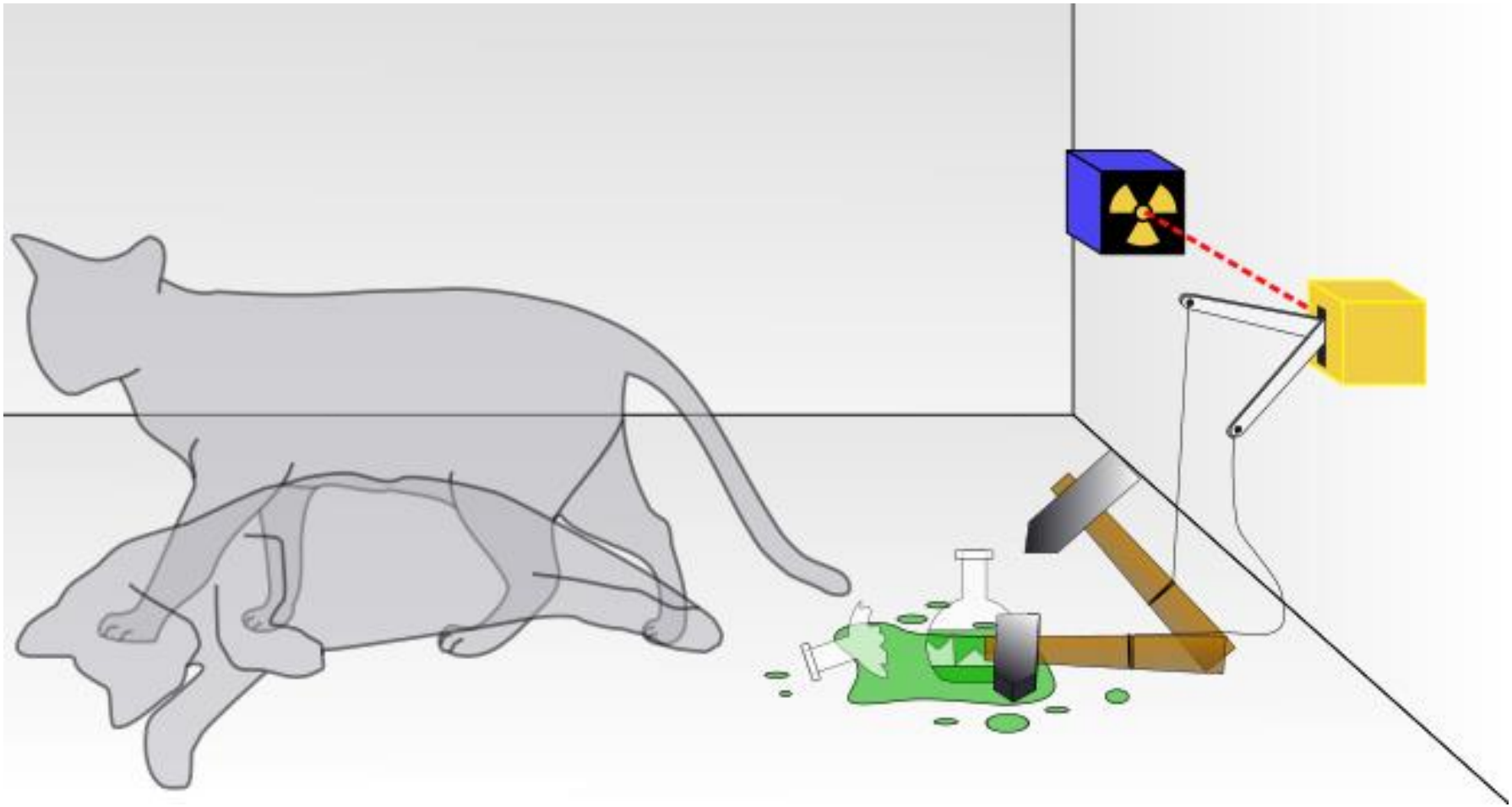


Einstein–Podolsky–Rosen-ov paradoks

1935

Viri slik: wikipedia

Schrödingerjeva mačka



Dhatfield - Own work, vir: wikipedia (https://en.wikipedia.org/wiki/Schrödinger‘s_cat)

Kvantna mehanika

Razmislimo abstraktno o dogodku z N možnimi izidi. Verjetnosti vseh izidov lahko zapišemo z vektorjem N realnih števil :

$$(p_1,....,p_N)$$

Kaj lahko povemo o tem vektorju?

- verjetnosti so nenegativne: $p_i \geq 0$
- njihov seštevek je 1.

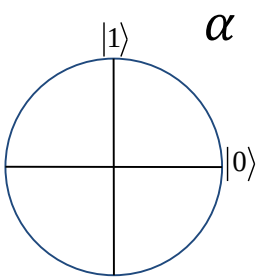
Zadnjo dejstvo lahko izrazimo s pomočjo prve norme: 1-norma vektorja verjetnosti mora biti 1 (1-norma je seštevek absolutnih vrednosti)

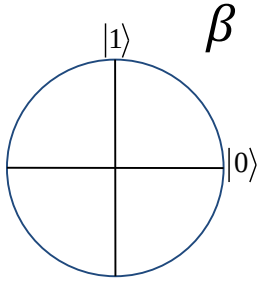
Ampak 1-norma ni edina norma na svetu - to ni edini način opredelitve "velikosti " vektorja. Obstajajo tudi drugi načini, in eden od najpogosteje uporabljenih, vsaj od Pitagorovih dni, je druga norma (**2-norma**) ali **Evklidska norma**.

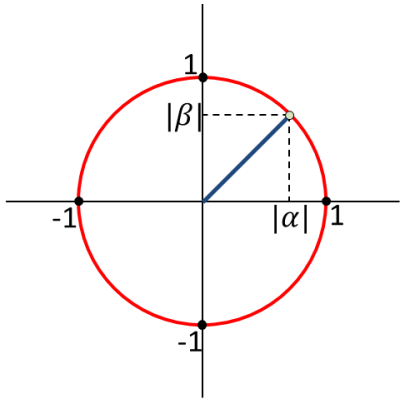
Negativne verjetnosti

Obravnavajmo en sam bit. V verjetnostnem računu lahko bit opišemo z dvema izidoma 0 in 1: bit zavzame vrednost 0 z verjetnostjo *p* in vrednost 1 z verjetnostjo 1-*p*.

Če pa namesto **1-norme** uporabimo **2-normo**, ne želimo več seštevati števil ampak njihove kvadratne vrednosti (Pitagorov izrek), njihov seštevek pa mora biti 1. Z drugimi besedami, želimo vektor (α,β) kjer $|\alpha|^2 + |\beta|^2 = 1$. Množica vseh takšnih vektorjev tvori krog v ravnini.







Toda zakaj v tem primeru ne pozabimo na α in β in samo opišemo stanje bita neposredno v smislu verjetnosti? Razlika nastopi pri transformaciji vektorja oz. v tem kako se vektor spremeni, ko ga vstavimo v linearno operacijo.

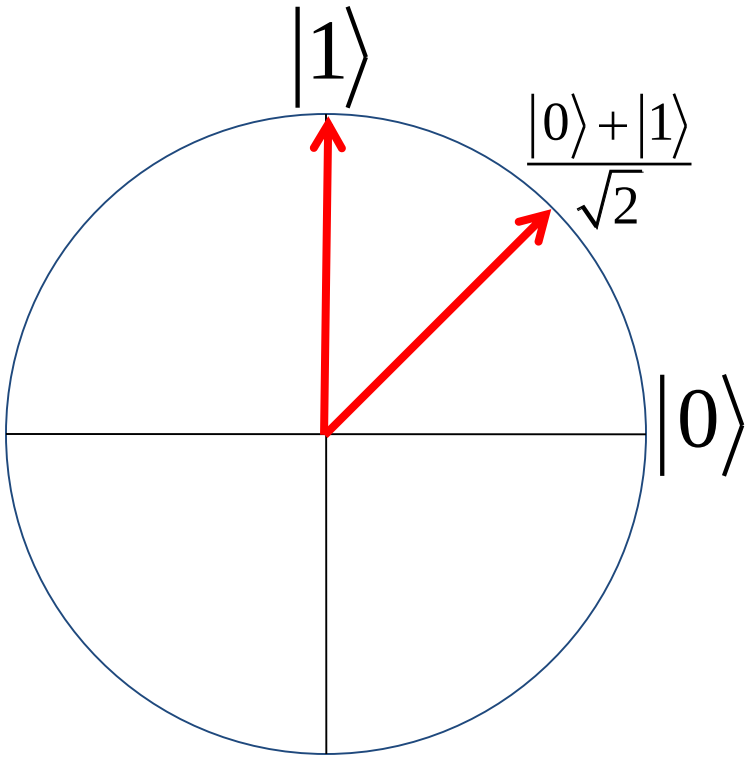
Kvantna mehanika & kvantni bit

Če je objekt lahko v dveh stanjih $|0\rangle$ ali $|1\rangle$, potem je lahko tudi **superpoziciji** teh stanj

$$\alpha|0\rangle + \beta|1\rangle$$

Tu sta α in β kompleksni **amplitudi verjetnosti**

$|\alpha|^2+|\beta|^2=1$



Če opazujemo ta objekt, bomo videli

$|0\rangle$ z verjetnostjo $|\alpha|^2$

$|1\rangle$ z verjetnostjo $|\beta|^2$

Takoj ko objekt pogledamo, le ta **kolapsira** v katerokoli izmed obeh osnovnih stanj, $|0\rangle$ ali $|1\rangle$.

Negativne verjetnosti

“Enotski vektor 2-norme" se imenuje kvantni bit (***qubit***) in fiziki ga navadno predstavijo s "**Diracovo ket notacijo**" v kateri vektor (α,β) postane **α|0⟩ + β|1⟩**.

- α je ***amplituda verjetnosti*** izida|0⟩,
- β je ***amplituda verjetnosti*** izida |1⟩.

Analogno lahko vsak kvantni bit predstavimo v dvodimenzionalnem vektorskem prostoru kot

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

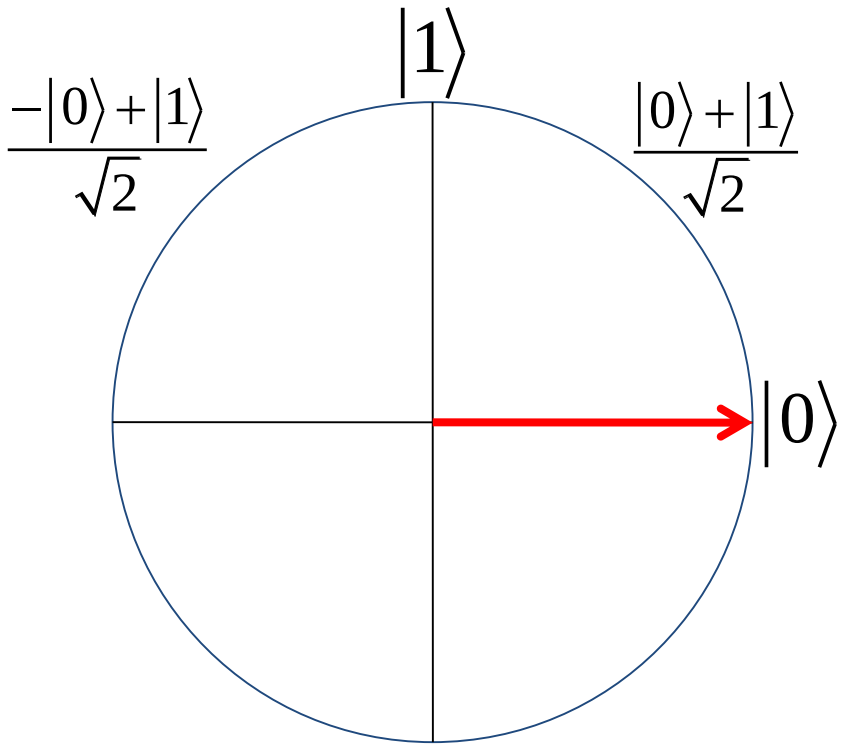
Potem lahko vsak kvanti bit s katerokoli unitarno matriko velikosti 2×2 pretvorimo v nov kvantni bit. Slavno kvantno interferenco lahko na primer zapišemo z Hadamardovo matriko **H**

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

Privzemimo, da je kvantni bit v stanju |0⟩. Če ga pomnožimo z zgornjo matriko **H** dobimo 1/√2(|0⟩ + |1⟩). Če ta rezultat še enkrat pomnožimo z **H** dobimo |0⟩

Kvantne transformacije: Hadamardova transformacija

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

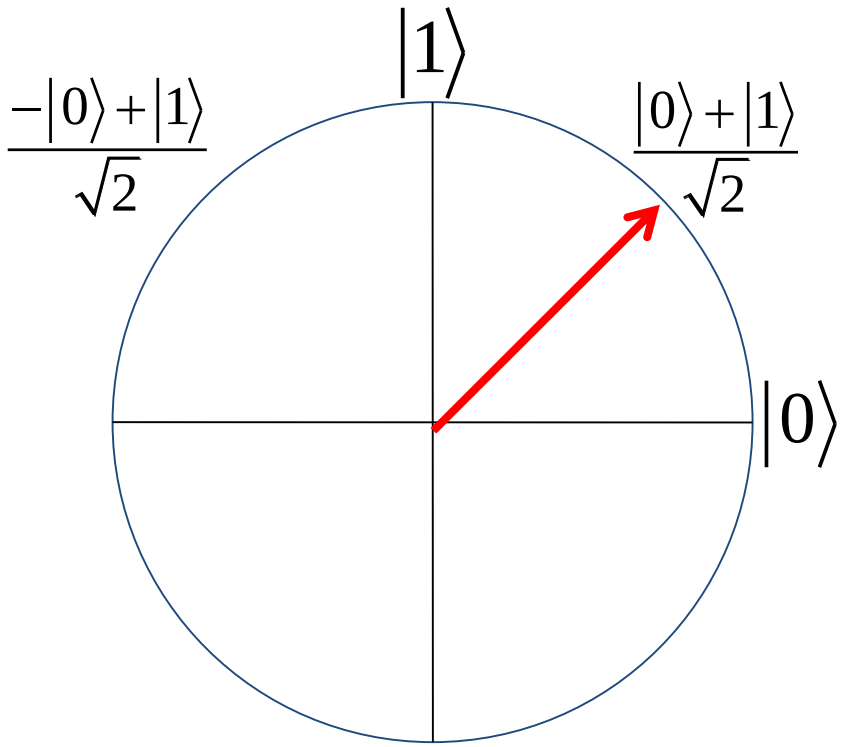


$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

Hadamardova transfromacija implementira **interferenco** amplitud verjetnosti — vir vse “kvantne čudaškosti”

Kvantne transformacije: Hadamardova transformacija

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

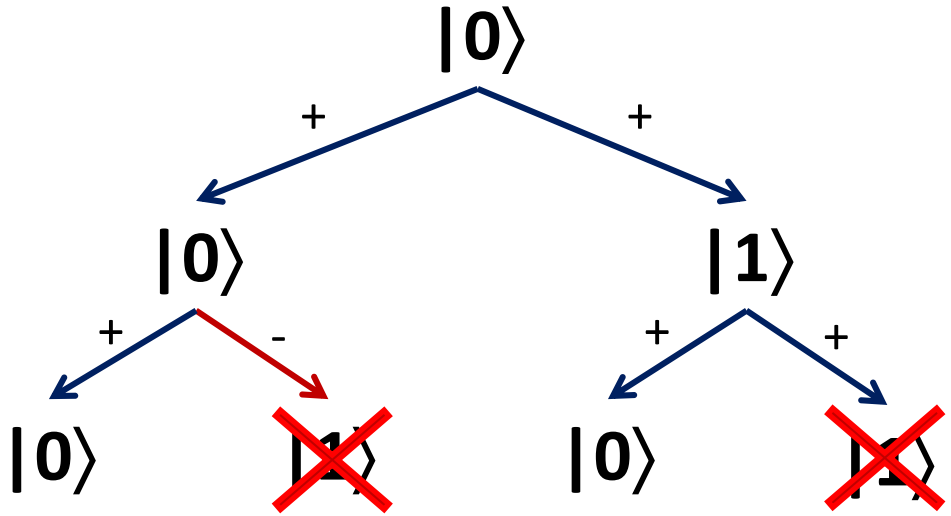


$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Hadamardova transfromacija implementira **interferenco** amplitud verjetnosti — vir vse “kvantne čudaškosti”

Negativne verjetnosti

Čeprav sta v obravnavani matriki **H** dve poti, ki vodita do izida |1⟩, ima ena pot pozitivno amplitudo verjetnosti, druga pa negativno amplitudo verjetnosti. Zaradi tega obe poti ***destruktivno interferirata*** is se medsebojno izničita. Poti ki vodita do izida|0⟩ imata obe pozitivni amplitudi verjetnosti in ***interferirata konstruktivno***.



Izničenje pozitivnih in negativnih amplitud verjetnosti poti, ki vodijo k določenem izidu je izvor vseh “kvantnih čudes" in tista lastnost, ki predstavlja glavno razliko med klasično in kvantno verjetnostjo.

Quantum Computing Since Democritus
(http://scottaaronson.com/democritus/default.html)

Zakaj 2-norma?

- Vzemimo teorijo, ki temelji na p-normi kjer je $p \epsilon \{1,2\}$.
- Vektor $(v_1,...,v_N)$ je *enotski vektor p-norme* če $|v_1|^p+...+|v_N|^p = 1$.
- Poiščimo linearno transformacijo, ki preslika katerikoli enotski vektor p-norme v drug enotski vektor p-norme.
- Za katerikoli izbrani p lahko najdemo linearne transformacije, ki ohranijo p-norm:
  - lahko na primer permutiramo elemente vektorja
  - lahko vstavimo negativne predznake.
- Toda, ***če poleg teh trivialnih trasformacij obstaja še katerakoli druga linearna trasformacija, ki ohranja p-normo, potem je p=1 ali p=2***.
  - če p=1, dobimo klasični verjetnostni račun,
  - če p=2 dobimo kvantno verjetnost (amplitudo verjetnosti).

Quantum Computing Since Democritus
(http://scottaaronson.com/democritus/default.html)

Realna vs. kompleksna števila

- Amplitude verjetnosti kvantne mehanike so kompleksna števila. To pomeni, da moramo kvadrirati absolutne vrednosti amplitud, da dobimo verjetnost. Z drugimi besedami, če je amplituda verjetnosti za nek izid $\alpha = \beta + \gamma i$, kjer sta β in γ realni števili, potem je verjetnost tega izida enaka $|\alpha|^2 = \beta^2 + \gamma^2$.
- ***Vprašanje**: Zakaj je narava izbrala kompleksna števila in ne realna*?
- **Odgovor**: Kompleksna števila so algebrajsko zaprta. Z drugimi besedami, za katerokoli linearno transformacijo U, obstaja linearna transformacija V tako da velja $V^2 = U$.

  Zgoraj podana relacija v bistvu definira ***zveznost***: če je smiselno, da operacijo izvedemo za časovni interval ene sekunde, mora biti smiselno tudi, da jo izvedemo za interval pol sekunde…

Quantum Computing Since Democritus
(http://scottaaronson.com/democritus/default.html)

Zakaj linearne transformacije?

- Abrams and Lloyd,1998 [1]: "***if* quantum mechanics were nonlinear, then one could build a computer to solve NP-complete problems in polynomial time"**.
- Torej bi lahko, če bi bila kvantna mehanika nelinearna, v polinomskem času izračunali karkoli

KARKOLI!

- Torej, ali je naš svet linearen ali pa lahko vnaprej napovemo/izračunamo katerikoli dogodek na svetu, od gibanja delnic, do življenjske dobe človeka in njegove svobodne volje...

[1] D. S. Abrams, S. Lloyd: Nonlinear quantum mechanics implies polynomial-time solution for NP-complete and #P problems, Phys.Rev.Lett. 81 (1998) 3992-3995

Quantum Computing Since Democritus
(http://scottaaronson.com/democritus/default.html)

Izjave o kvantni mehaniki

- "Basically, *quantum mechanics is the operating system that other physical theories run on as application software* (with the exception of general relativity, which hasn't yet been successfully ported to this particular OS)"
- "it's not about matter, or energy, or waves, or particles - it's about information and probabilities and observables, and how they relate to each other".

"Quantum mechanics is what you would inevitably come up with if you started from probability theory, and then said, let's try to generalize it so that the numbers we used to call "probabilities" can be negative numbers. As such, the theory could have been invented by mathematicians in the 19th century without any input from experiment. It wasn't, but it could have been."

Scott Aaronson

Quantum Computing Since Democritus
(http://scottaaronson.com/democritus/default.html)

Tenzorski produkt

- Če poznamo stanji dveh kvantnih bitov, potem lahko njuno **kombinirano stanje** zapišemo s **tensorskim produktom**:

- **primer**
  - če je prvi kvanti bit: $\alpha|0\rangle+\beta|1\rangle$
  - in drugi kvantni bit: $\gamma|0\rangle+\delta|1\rangle$
  - potem njuno kombinirano stanje zapišemo kot

$$(\alpha|0\rangle+\beta|1\rangle) \otimes (\gamma|0\rangle+\delta|1\rangle) = \alpha\gamma|00\rangle+\alpha\delta|01\rangle+ \beta\gamma|10\rangle+\beta\delta|11\rangle$$

Ločljiva vs. prepletena stanja

- **Ločljiva stanja**: stanja dveh ali več kvantnih bitov, ki jih lahko zapišemo kot tenzorski produkt posameznih kvantnih bitov.
- **Prepletena stanja:** stanja dveh ali več kvantnih bitov, ki jih ne moremo zapisati kot tenzorski produkt posameznih kvantnih bitov. Najbolj slavno prepleteno stanje para kvantnih bitov je stanje EPR (Einstein-Podolsky-Rosen) :

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

- **Formalna definicija**: Če lahko kombinirano stanje ρ dveh podsistemov A in B, ki sta v stanjih $|\psi_A\rangle$ in $|\psi_B\rangle$, zapišemo z verjetnostno porazdelitvijo tenzorskega produkta stanj $\alpha|\psi_A\rangle \otimes \beta|\psi_B\rangle$, potem je ρ **ločljivo** stanje. V nasprotnem primeru je ρ ***prepleteno*** stanje. V zgornjem primeru sta α in β amplitudi verjetnosti.

https://www.youtube.com/watch?v=O8Ia3kcQydc

Dr Quantum - entanglement (youtube)

Teorem neizvedljivosti kloniranja

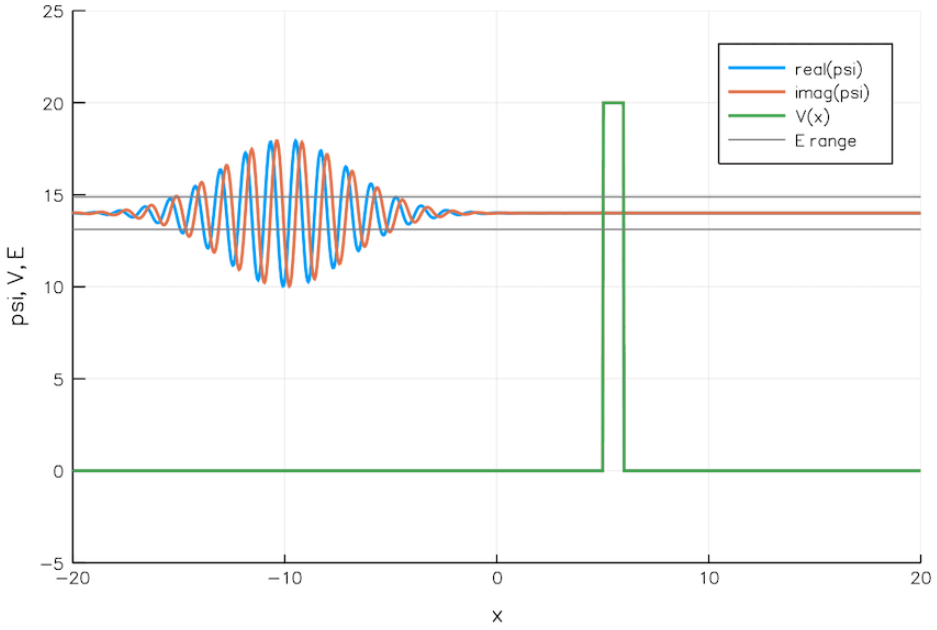
(No-cloning theorem)

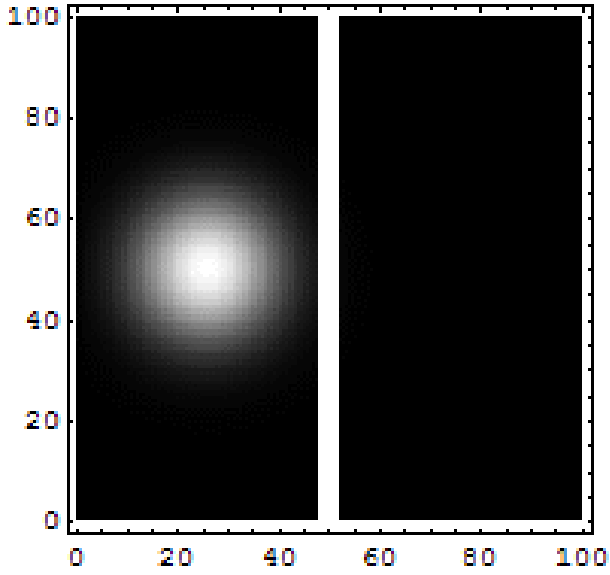
- prepoveduje kloniranje identičnih kopij poljubnega kvantnega stanja
- zagotovljen je s strani linearnosti kvantne mehanike.
- Posledice:
  - ne moremo izdelati varnostnih (backup) kopij kvantnega stanja in jih med kvantnim izračunom uporabiti za odpravo računskih napak oz. za odkrivanje rešitev sistema enačb (Shorov algoritem).
  - omogoča varno izmenjavo ključev: prisluškovalec ne more izdelati kopije poslanega kvantnega kriptografskega ključa.

Kvantno tuneljenje

(Quantum tunneling)

- **Klasična mehanika**: delci, ki nimajo dovolj energije, da bi prešli oviro, je ne bodo nikoli prešli.
- **Kvantna mehanika**: Ti delci lahko z zelo majhno verjetnostjo preidejo na drugo stran ovire. Pojavu pravimo kvantno tuneljenje.





https://en.wikipedia.org/wiki/Quantum_tunnelling

quantum tunneling (youtube)

Richard Feynman

Kvantno računalništvo

(quantum computing)

Richard Feynman (1982). "Simulating physics with computers". *International Journal of Theoretical Physics* **21**: 467.

Klasična predstavitev podatkov

- Osnovna enota klasičnih podatkov je bit, ki lahko zavzame vrednosti 0 ali 1.
- Klasični računalnik predstavi podatke kot niz bitov.
- Črko ‘A’ zapišemo kot 0100 0001
- Število 165 zapišemo kot 1010 0101

binarne kode:

$10100101_2 =$

$1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 =$

$1 \cdot 128 + 0 \cdot 64 + 1 \cdot 32 + 0 \cdot 16 + 0 \cdot 8 + 1 \cdot 4 + 0 \cdot 2 + 1 \cdot 1 =$

165_{10}

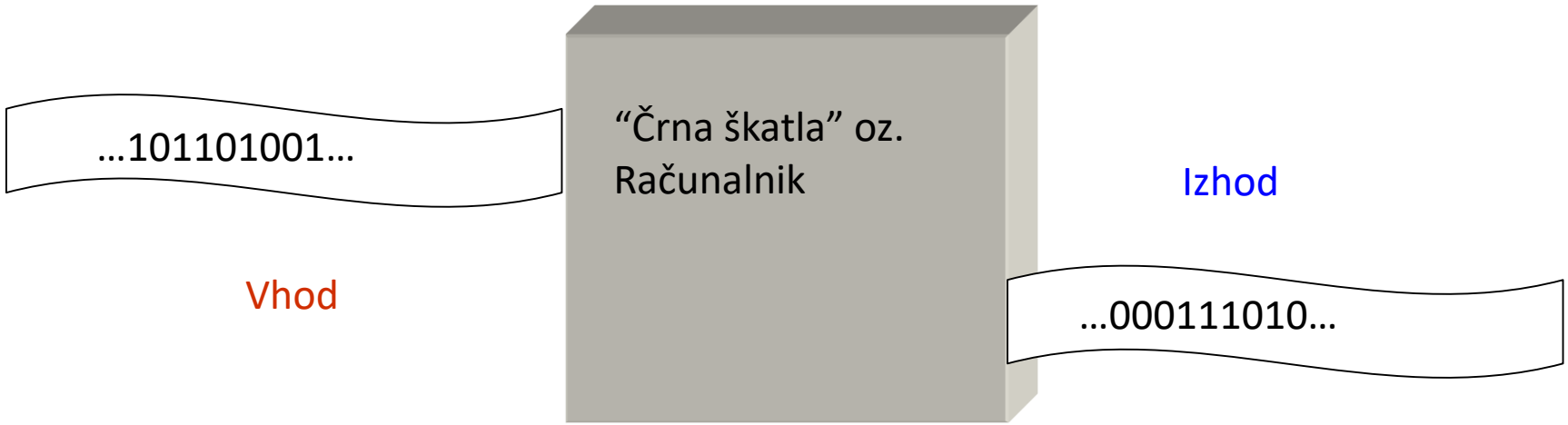
Klasične operacije

- Vse operacije temeljijo na logičnih vratih.

- Na primer, logična vrata IN (AND) sprejmejo dva vhodna bita in vrnejo 1, če in samo če sta oba vhoda na 1.

Klasični algoritem

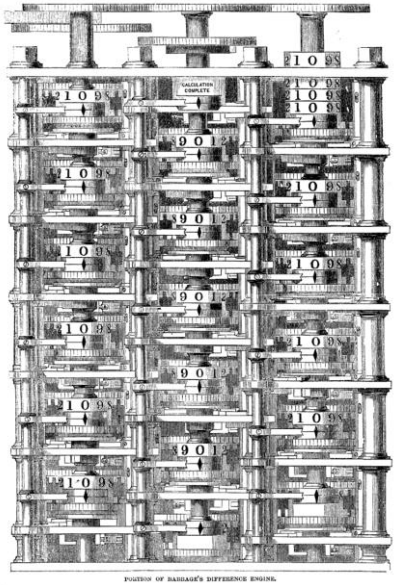
- Klasični algoritem je vsako zaporedje klasičnih operacij.
- Klasičen računalnik je vsaka naprava, ki lahko implementira klasični algoritem.



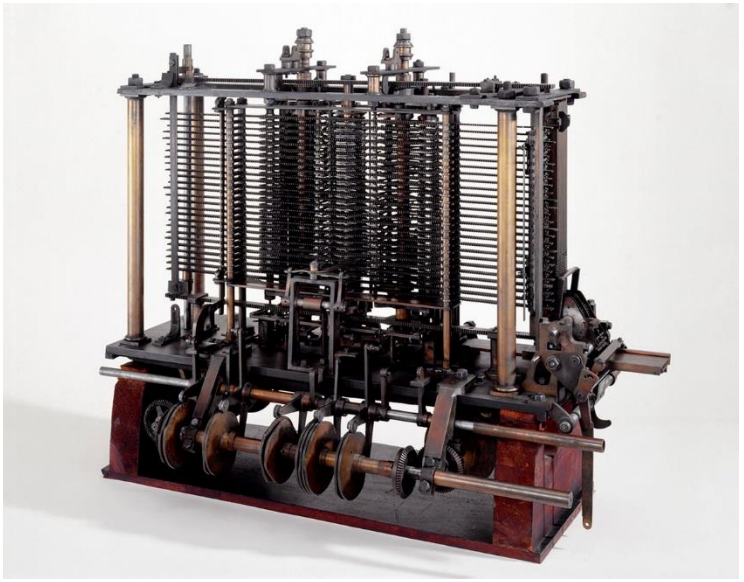
Klasični računalnik

- Čeprav moderni računalniki temeljijo na kvanti mehaniki (tranzistorjih), še vedno poganjajo klasične algoritme.
- V principu bi lahko izdelali klasični računalnik, ki ne bi temeljil na kvantni mehaniki (npr. mehanski stroj iz zobnikov).

Charles Babbage
(1791-1871)



https://en.wikipedia.org/wiki/Charles_Babbage#/media/File:Babbage_difference_engine_drawing.gif



https://en.wikipedia.org/wiki/Analytical_engine#/media/File:Babbages_Analytical_Engine,_1834-1871._(9660574685).jpg

Kaj torej je kvantni računalnik?

Kvantni računalnik

- Kvantni računalnik je računalnik, ki v izračunih neposredno uporablja lastnosti kvantnega sveta:
  - Superpozicija stanj
  - Prepletenost stanj
  - Kvantno tuneljenje
- S tem izrazno krepko razširi klasično računanje (veliko dodatnih prostostnih stopenj) in eksponentno pohitri iskanje rešitev.

- Številni problemi, ki imajo na klasičnem računalniku eksponentno računsko zahtevnost, so na kvantnem računalniku rešljivi v polinomskem času.

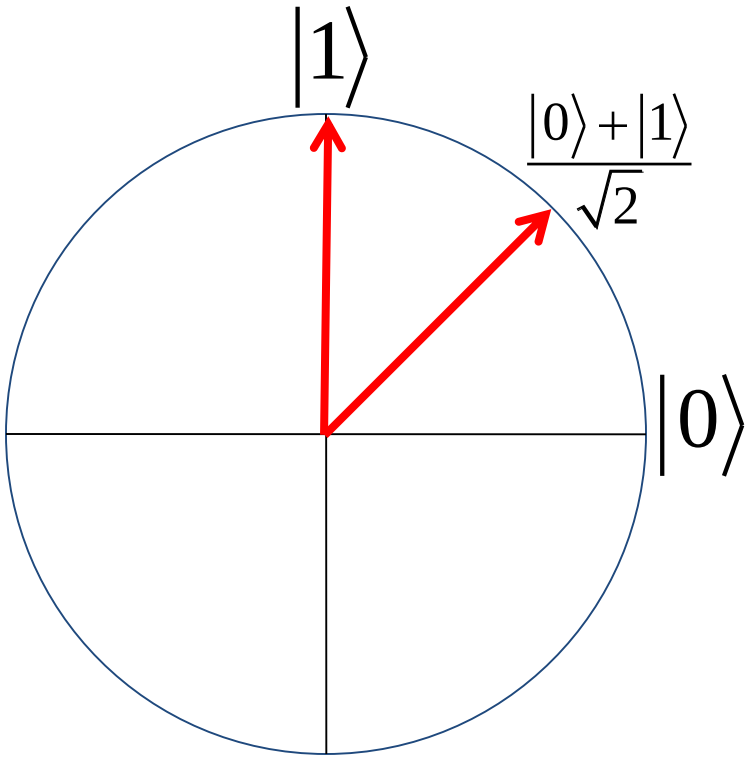
Kvantna mehanika & kvantni bit

Če je objekt lahko v dveh stanjih $|0\rangle$ ali $|1\rangle$, potem je lahko tudi **superpoziciji** teh stanj

$$\alpha|0\rangle + \beta|1\rangle$$

Tu sta α in β kompleksni **amplitudi verjetnosti**

$|\alpha|^2+|\beta|^2=1$



Če opazujemo t objekt, bomo videli

$|0\rangle$ z verjetnostjo $|\alpha|^2$

$|1\rangle$ z verjetnostjo $|\beta|^2$

Takoj ko objekt pogledamo, le ta **kolapsira** v katerokoli izmed obeh osnovnih stanj, $|0\rangle$ ali $|1\rangle$.

Kvantni biti

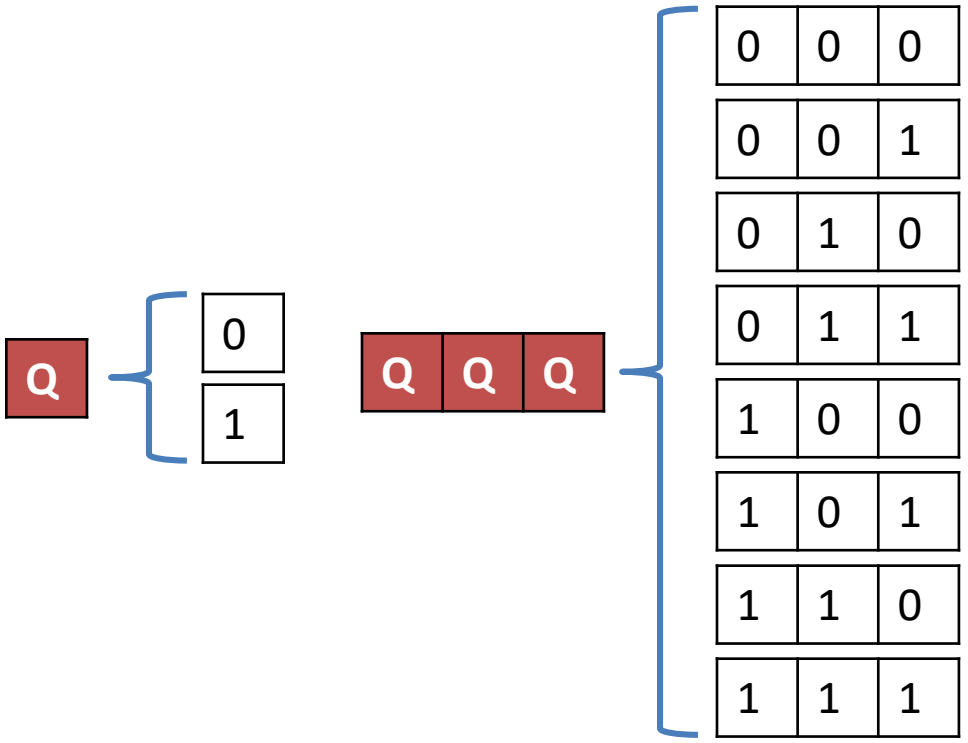
- Za razliko od klasičnega bita, ki je zagotovo v enem od dveh stanj, je stanje kvantnega bita v splošnem mešanica obeh stanj |0> in |1>.

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

- Amplitudi verjetnosti sta normirani (2-norma):

$$|\alpha|^2 + |\beta|^2 = 1$$

Kvantni register



100 kvantnih bitov lahko hrani več klasičnih bitov informacij kot je atomov v znanem vesolju!

Kvantni register: superpozicija

- zbir n kvantnih bitov:

$$|\mathbf{a}\rangle = |a_{n-1}\rangle \otimes |a_{n-2}\rangle \ldots |a_1\rangle \otimes |a_0\rangle$$

- **primeri**:
  - $|\mathbf{3}\rangle = |0\rangle \otimes |1\rangle \otimes |1\rangle = |011\rangle$
  - $|\mathbf{7}\rangle = |1\rangle \otimes |1\rangle \otimes |1\rangle = |111\rangle$
  - $|\mathbf{21}\rangle = |1\rangle \otimes |0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle = |10101\rangle$
  - $\mathbf{1/\sqrt{2}\,(|3\rangle + |7\rangle)} = 1/\sqrt{2}\,(|0\rangle + |1\rangle) \otimes |1\rangle \otimes |1\rangle$
  - $2^{-3/2}\,\mathbf{(|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle) =}$

$$1/\sqrt{2}\,(|0\rangle + |1\rangle) \otimes$$
$$1/\sqrt{2}\,(|0\rangle + |1\rangle) \otimes$$
$$1/\sqrt{2}\,(|0\rangle + |1\rangle)$$

Kvantna vrata

- Kvantna logična vrata implementirajo unitarno transformacijo stanja enega ali več kvantnih bitov v novo stanje kvantnih bitov.
- predstavimo jih lahko kot linearne operatorje v Hilbertovem prostoru.
- **Nelinearne transformacije so PREPOVEDANE!**
- Kvanta vrata je najprimerneje predstaviti z matrikami, kjer stanje posameznega kvantnega bita zapišemo v bazi stanj $|0\rangle$ in $|1\rangle$:

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

Kvantna vrata & unitarna matrika

Stanje

$$\sum_{i=1}^{n} \alpha_i \left| i \right\rangle$$

spremenimo tako, da ga predmnožimo z **unitarno** matriko — takšno matriko, ki ohranja relacijo.

$$\sum_{i=1}^{n} \left| \alpha_i \right|^2 = 1$$

Kvantna vrata NOT

- Kot pri klasičnem računanju, kvantna vrata NOT vrnejo $|0\rangle$, če je vhod $|1\rangle$ in $|1\rangle$, če je vhod $|0\rangle$.
- Matrična predstavitev vrat NOT:

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

zgornja matrika je podana v bazi:

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

Kvantna vrata NE

- Kot pri klasičnem računanju, kvantna vrata NOT vrnejo $|0\rangle$, če je vhod $|1\rangle$ in $|1\rangle$, če je vhod $|0\rangle$:

$$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix}=\begin{bmatrix}0\\ 1\end{bmatrix} \qquad \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix}=\begin{bmatrix}1\\ 0\end{bmatrix}$$

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

- Rezultat postane zanimiv, ko vrata uporabimo nad superpozicijo stanj

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

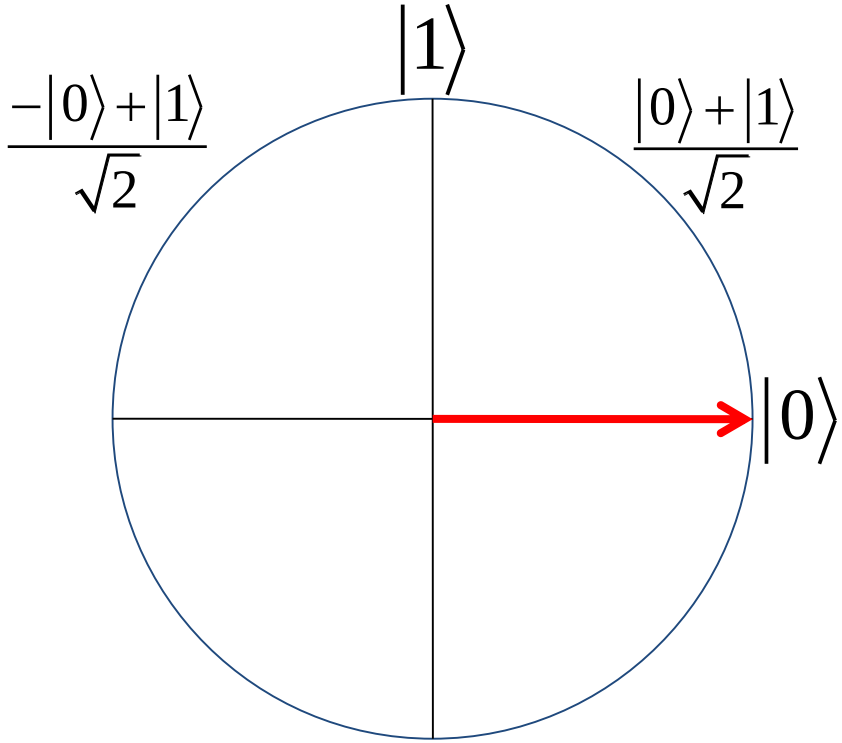
- V tem primeru vrata NE zamenjajo amplitudi verjetnosti kvantnega bita!

Kvantna vrata: Hadamard-ova vrata

- prejmejo en sam vhodni kvantni bit

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

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

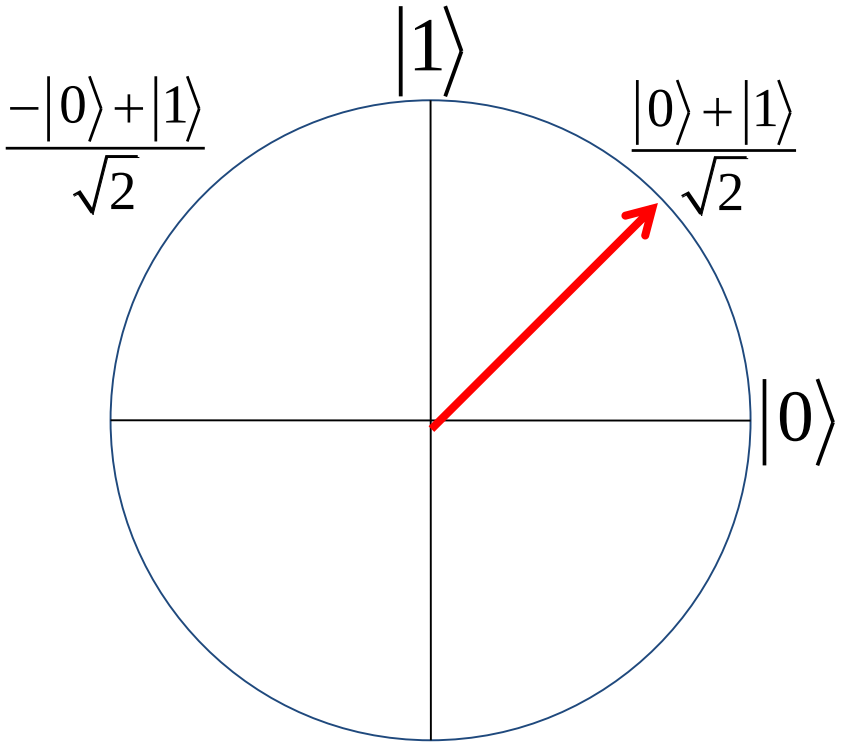


Kvantna vrata: Hadamard-ova vrata

- prejmejo en sam vhodni kvanti bit

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

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

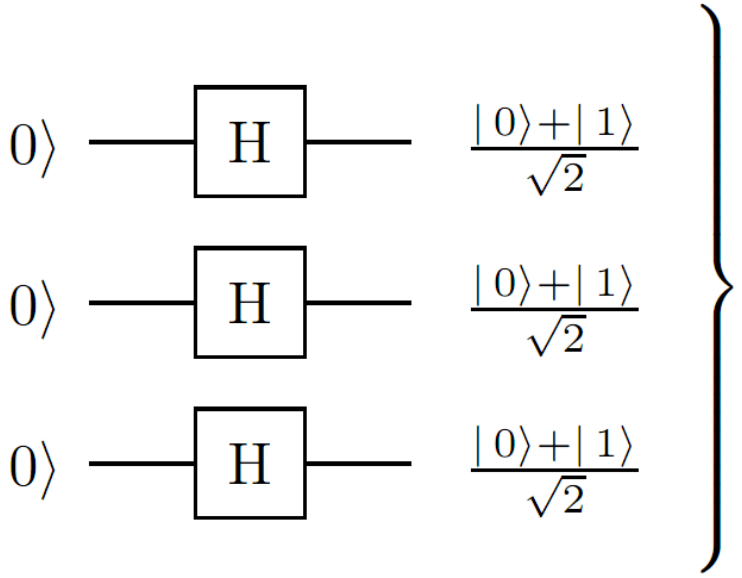


Kvantna vrata: Hadamard-ova vrata

- H je sama sebi inverz: $\mathbf{H} = \mathbf{H}^T = \mathbf{H}^{-1}$

$$\mathbf{H}\cdot\mathbf{H} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\cdot\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$

- aplikacija na več kvantnih bitov:



IN BINARY

$$= \frac{1}{2^{3/2}}\left\{\begin{array}{l}|000\rangle + |001\rangle + |010\rangle + |011\rangle + \\ + |100\rangle + |101\rangle + |110\rangle + |111\rangle\end{array}\right\}$$

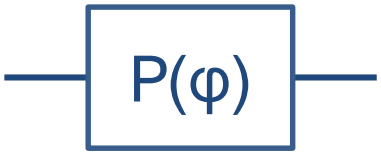
$$= \frac{1}{2^{3/2}}\left\{\begin{array}{l}|0\rangle + |1\rangle + |2\rangle + |3\rangle + \\ + |4\rangle + |5\rangle + |6\rangle + |7\rangle\end{array}\right\}$$

IN DECIMAL

Kvantna vrata: Fazna vrata

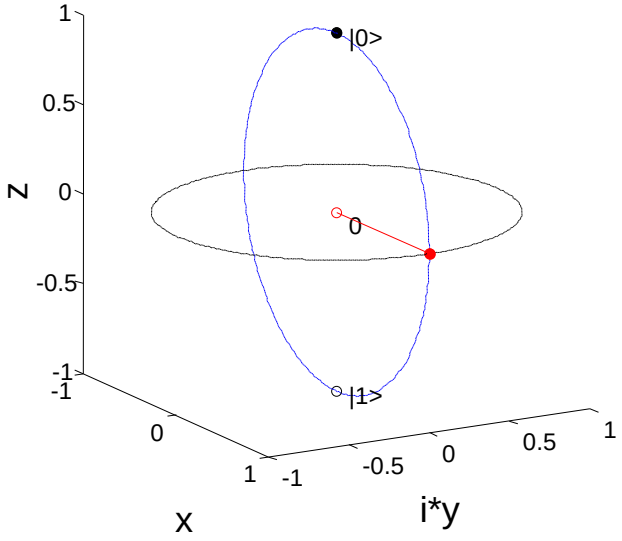
- prejmejo en vhodni kvantni bit

$$P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$



$$\varphi = 0 \Rightarrow P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

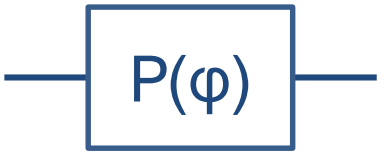
$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$



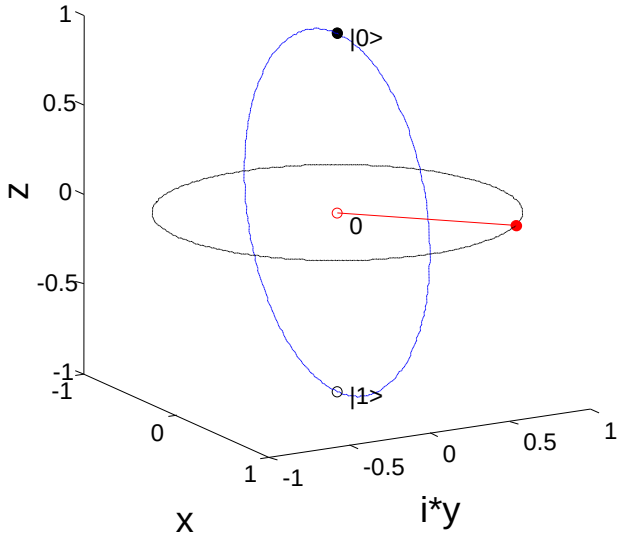
Kvantna vrata: Fazna vrata

- prejmejo en vhodni kvantni bit

$$P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$



$$\varphi = \frac{\pi}{4} \Rightarrow P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}} \end{bmatrix}$$



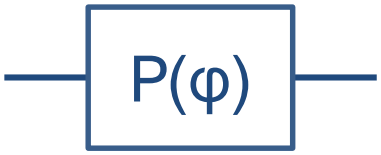
$$\begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

$$= \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{2} + i\frac{1}{2} \end{bmatrix}$$

Kvantna vrata: Fazna vrata

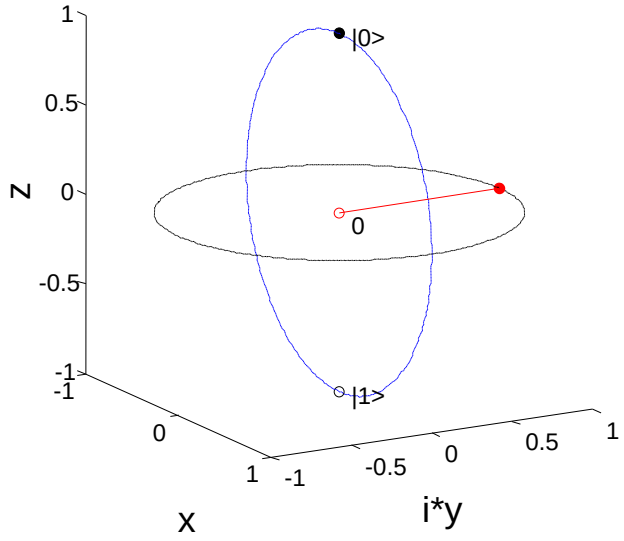
- prejmejo en vhodni kvantni bit

$$P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$



$$\varphi = \frac{\pi}{2} \Rightarrow P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

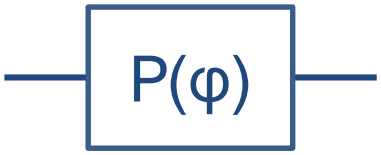
$$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ i\frac{1}{\sqrt{2}} \end{bmatrix}$$



Kvantna vrata: Fazna vrata

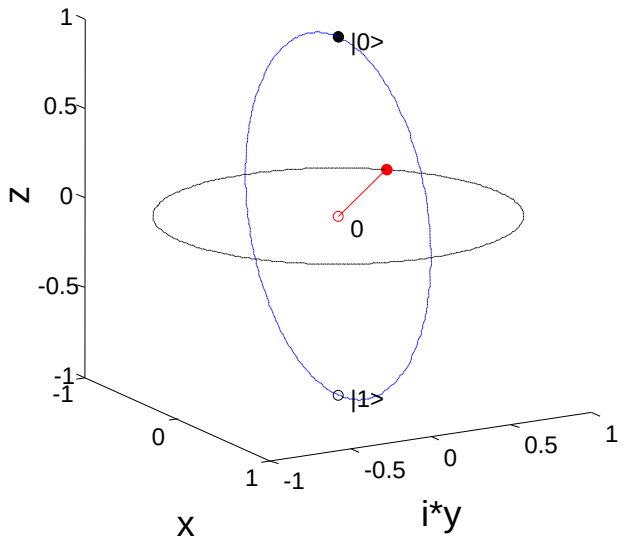
- prejmejo en vhodni kvantni bit

$$P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$



$$\varphi = \frac{3\pi}{4} \Rightarrow P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & -\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}} \end{bmatrix}$$

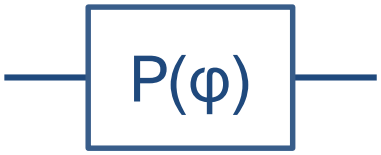
$$\begin{bmatrix} 1 & 0 \\ 0 & -\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{2} + i\frac{1}{2} \end{bmatrix}$$



Kvantna vrata: Fazna vrata

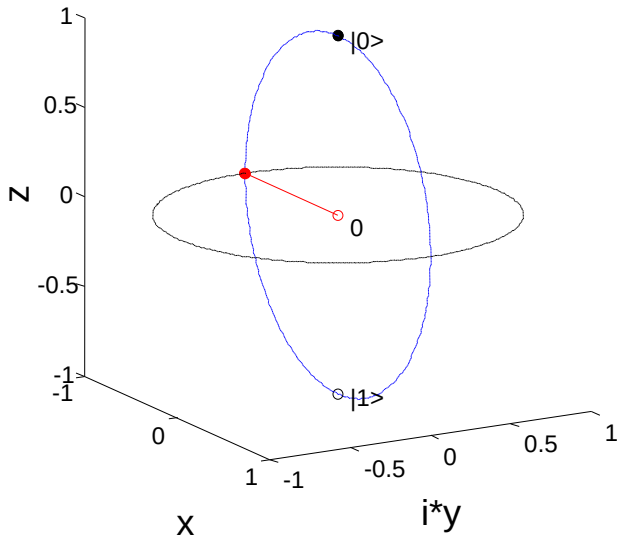
- prejmejo en vhodni kvantni bit

$$P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$



$$\varphi = \pi \Rightarrow P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

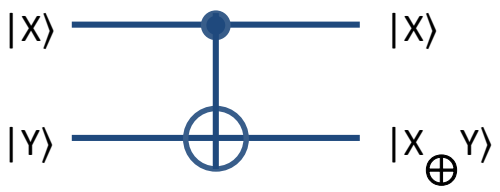
$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix}$$



Kontrolirana NE vrata (Controlled-NOT)

- prejmejo dva kvantna bita, implementirajo XOR

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



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

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

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

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

Kvantna prepletenost in Bellovo stanje

- Dana sta dva kvantna bita. Oba sta v stanju $|0\rangle$:

$$|0\rangle, |0\rangle$$

- Nad prvim bitom uporabimo Hadamardova vrata:

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, |0\rangle$$

- Tvorimo tenzorski produkt obeh kvantnih bitov:

$$\frac{1}{\sqrt{2}}|00\rangle + 0|01\rangle + \frac{1}{\sqrt{2}}|10\rangle + 0|11\rangle$$

- Nad registrom uporabimo vrata CNOT

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}|00\rangle + 0|01\rangle + 0|10\rangle + \frac{1}{\sqrt{2}}|11\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

- To stanje imenujemo Bellovo stanje (po fiziku John Stewart Bell-u iz Severne Irske) ali stanje ERP (Einstein, Podolsky & Rosen).

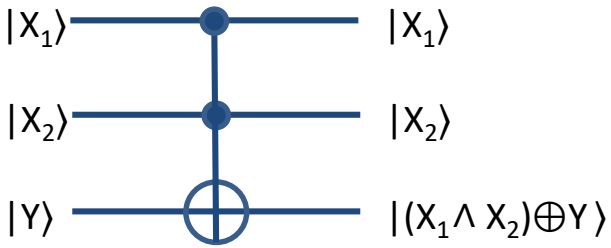
Kvantna prepletenost in Bellovo stanje

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

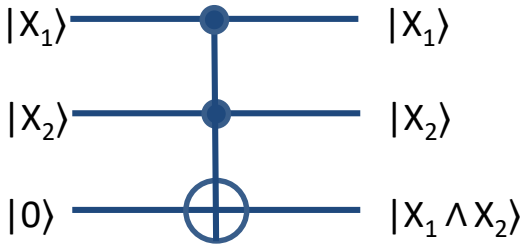
- Bellovega stanja ali stanja ERP ne moremo faktorizirati v tenzorski produkt posameznih kvantnih bitov (poskusite sami!).
- Pravimo, da je stanje kvantno prepleteno. Ko register izmerimo, dobimo s 50% verjetnostjo klasično vrednost 00, s 50% pa klasično vrednost 11. Kvantna bita sta torej prepletena in meritev enega pove vrednost drugega. Če izmerimo prvega in dobimo vrednost 0, potem je tudi drugi v vrednosti 0. Če pa je po meritvi prvi bit v vrednosti 1, je v vrednosti 1 tudi drugi bit.
- Zanimivost kvantnega prepleta je, da lahko bita ločimo v prostoru, pa bosta še vedno oba odreagirala na meritev enega.
- To pa ni edino možno Bellovo stanje. Vsa možna Bellova stanja dobimo, če na začetku predstavljenega vezja nastavimo vrednosti kvantnih bitov na $|00\rangle$, $|01\rangle$, $|10\rangle$ in $|11\rangle$.

Dvojna kontrolirana NE vrata: c^2-NOT ali Toffoli

- c^2-NOT ali vrata Toffoli:

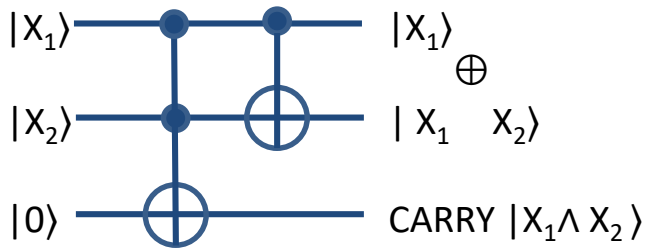


- reverzibilna vrata AND ($|y\rangle$ postavimo na $|0\rangle$):



Kvantna vrata: Univerzalen nabor

- S kvantnimi vrati NOT, AND in C-NOT lahko ovrednotimo katerokoli Booleovo funkcijo $\{0, 1\}^n \rightarrow \{0, 1\}^m$, ki preslika *n* vhodnih kvantih bitov v *m* izhodnih kvantnih bitov.
- Ni nujno, da je takšno vezje učinkovito (merjeno v številu vrat, ki ga sestavljajo).



KVANTNO SEŠTEVANJE

Kvantna vrata: Literatura

Lep pregled kvantnih vrat, njihovih simbolov in njihovih unitarnih matrik najdete na Wikipediji:

- https://en.wikipedia.org/wiki/List_of_quantum_logic_gates