

Kvantno računanje

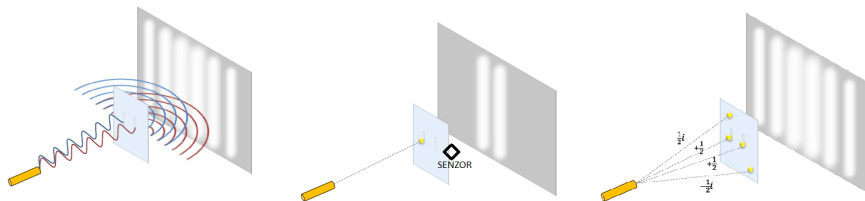
Andrea Ažman

April 2022

1 Uvod

Najbolj znan eksperiment kvantne mehanike je zagotovo eksperiment z dvojno rezo, ki demonstrira dualno naravo svetlobe. Svetloba se včasih obnaša kot valovanje, včasih pa kot fotoni. Če gledamo na svetlobo kot na valovanje, bo za režama nastal interferenčni vzorec, saj se bo svetloba skozi reži širila v krogih (leva slika spodaj). Če pa na svetlobo gledamo kot na skupek kvantnih delcev oziroma fotonov, bo za režama nastal odsev obeh rež (srednja slika spodaj).

Rezultat je odvisen od meritve. Takoj ko izmerimo skozi katero rezo je po toval foton, interferenčni vzorec izgine. Odločilnega pomena je torej meritev oziroma dodatni senzor. Če tega dodatnega senzorja ne bi imeli in bi vseeno "streljali" fotone posamično, bi vseeno nastal interferenčni vzorec, saj bi posamezni foton šel hkrati skozi obe reži in interferiral sam s sabo. Še več, delec je istočasno šel skozi eno in drugo rezo, skozi obe in skozi nobeno (desna slika spodaj). Ko pa delec izmerim, kje je, se obnaša kot klasični delec.



2 Klasični računalniki in logična vrata

Osnovna enota klasičnih podatkov je bit. Zavzame lahko vrednosti 0 ali 1. Klasični računalnik predstavi podatke kot niz bitov, na primer:

- Črko A zapišemo z zaporedjem 01000001.
- Število 165 zapišemo z zaporedjem 10100101.

Računske operacije klasičnega računalnika potekajo preko logičnih vrat (logičnih operatorjev). Logična vrata sprejmejo dva vhodna bita in vrnejo enega. Iz pravilnostne tabele sledi, da je pri logičnih vratih IN izhod 1, če in samo če sta oba vhoda 1. Pri logičnih vratih ALI je izhod 1, če je vsaj eden od vhodov 1. Logična vrata NE sprejmejo samo en vhodni bit in izhod je negirana vrednost vhoda.

3 Postulati kvantne mehanike

Najpreprostejši kvantni sistem je *kubit*. To je sistem z dvema ločenima stanjema $|0\rangle$ in $|1\rangle$.

Imejmo kvantni sistem s k končnimi stanji. Ta končna stanja imenujemo *bazna stanja* in jih označimo z $|0\rangle, |1\rangle, \dots, |k-1\rangle$. Kvantni sistem je lahko v več stanjih hkrati. Pravimo, da je lahko v poljubni *superpoziciji*.

1. Načelo superpozicije: Stanje kvantnega sistema opišemo z enotskim vektorjem v prostoru stanj $\mathcal{H}$, ki je kompleksni vektorski prostor s skalarnim produktom, v katerem bazna stanja $|0\rangle, |1\rangle, \dots, |k-1\rangle$ tvorijo ortonormirano bazo.

Iz skalarnega produkta, definirane na tem prostoru, izhaja tudi uporabljen zapis. Imenuje se *Diracov zapis*, kjer vektorje zapisujemo kot $|\varphi\rangle$. Ta zapis se prebere kot *ket* φ .

Superpozicija je linearna kombinacija vseh stanj. Torej vektor, ki nam opiše stanje sistema, lahko izrazimo kot

$$|\varphi\rangle = \sum_{j=0}^{k-1} \alpha_j |j\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \dots + \alpha_{k-1} |k-1\rangle,$$

kjer so koeficienti $\alpha_j \in \mathbb{C}$, za katere velja $\sum_{j=0}^{k-1} |\alpha_j|^2 = 1$. Koeficientom α_j pravimo tudi *amplitude*. Njihove absolutne vrednosti nam povedo, kolikšen je delež posameznega stanja v superpoziciji.

Da našemu do sedaj definirane kvantnemu sistemu ne bo dolgčas, ga združimo s še enim sistemom. Poglejmo si združitev dveh kubitov. En kubit ima bazni stanji $|0\rangle$ in $|1\rangle$. V združenem sistemu potem ločimo štiri stanja in sicer $|00\rangle, |01\rangle, |10\rangle$ in $|11\rangle$. Torej ta sistem je lahko v superpoziciji oblike

$$\alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle.$$

Naj bo prvi kubit v stanju $|\varphi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ in drugi kubit v stanju $|\psi\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$. Nanju pogledimo kot na združen sistem. Njegovo stanje je potem enako tenzorskemu produktu

$$|\varphi\rangle \otimes |\psi\rangle = \alpha_0 \beta_0 |00\rangle + \alpha_0 \beta_1 |01\rangle + \alpha_1 \beta_0 |10\rangle + \alpha_1 \beta_1 |11\rangle.$$

Stanja, ki jih lahko zapišemo kot tenzorski produkt, imenujemo *produktna stanja*. Primer stanja, ki ni produktno, je *Bellovo stanje* $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$. Stanjem, ki niso produktna pa pravimo *prepletena*.

2. Združitev kvantnih sistemov: Prostor stanj sistema, ki ga dobimo z združitvijo sistemov s prostoroma stanj $\mathcal{H}$ in $\mathcal{H}'$, je enak tenzorskemu produktu $\mathcal{H} \otimes \mathcal{H}'$. Če je prvi sistem v stanju $|\varphi\rangle$ in drugi sistem v stanju $|\psi\rangle$, je združen sistem v stanju $|\varphi\rangle \otimes |\psi\rangle$.

Pri klasičnem računalništvu preslikave upodobimo s klasičnimi vezji, katera so sestavljena iz logičnih vrat. Kvantna vezja bodo predstavljala unitarne preslikave. Podobno kot logična vrata, bodo kvantna vrata sestavljala kvantno vezje. Torej kvantna vrata bodo predstavljala enostavnejše unitarne preslikave. V ponedeljek si bomo na predavanju pogledali *Paulijeva vrata*, *Hadamardova vrata* in *vrata kontrolirane negacije/CNOT VRATA*.

3. Unitarnost razvoja: *Za vsak razvoj izoliranega kvantnega sistema obstaja unitarna matrika U , ki začetno stanje $|\varphi_0\rangle$ slika v stanje po spremembi $U|\varphi_0\rangle$.*

Ker pa ni dovolj, da je kvantni sistem lahko v več stanjih hkrati, je za zabavo poskrbljeno tudi takrat, ko želimo izmeriti njegovo stanje. Na tem mestu bi uporabila prispodobo z navihanim otrokom. Predstavljajte si navihanega otroka, ki dela domačo nalogo. Seveda njemu to niti malo ne diši, zato poleg reševanja domače naloge počne še mnogo drugih reči (se igra s svinčnikom, riše in kraca, opazuje dogajanje skozi okno, ...). A ko otroka pogledamo, on lepo pridno sedi in rešuje, ali pa ga bomo zalotili pri eni od ostalih stvari, ki jih počne. Pri kvantnem sistemu je podobno. Vemo, da je v več stanjih hkrati, a ko ga bomo izmerili, bomo zaznali le eno od možnih stanj.

4. Načelo meritve: *Če merimo sistem v stanju $\sum_{j=0}^{k-1} \alpha_j |j\rangle$, z verjetnostjo $|\alpha_j|^2$ izmerimo stanje $|j\rangle$, po meritvi pa je stanje sistema enako $|j\rangle$.*

Naslednji izrek je pomemben predvsem pri kvantni kriptografiji. Prisluškovalec želi, da ostane neopažen pred sogovornikoma. V ta namen bi želel zakodirano sporočilo najprej podvojiti in dvojnik zadržati zase ter ga potem izmeriti. To pa ni možno, ker ne obstaja taka unitarna preslikava, s katero bi lahko podvojili stanje.

Izrek o podvajanju: *Ne obstaja unitarna preslikava U , za katero za vsako stanje enega kubita $|\varphi\rangle$ velja $U(|\varphi\rangle \otimes |0\rangle) = |\varphi\rangle \otimes |\varphi\rangle$.*

Izrek bomo skupaj dokazali na predavanjih. Meritev pa se mora uskladiti tudi na ravni združenega sistema, zato podajam še zadnji postulat.

5. Meritev v združenem sistemu: *Če je združen sistem v stanju $\sum_{j=0}^{k-1} \alpha_j |j\rangle \otimes |\psi\rangle$, kjer so vsi vektorji $|\psi_j\rangle$ enotski, potem pri meritvi prvega sistema z verjetnostjo $|\alpha_j|^2$ izmerimo stanje $|j\rangle$, po meritvi pa je stanje združenega sistema enako $|j\rangle \otimes |\psi_j\rangle$.*

Kot primer si bomo na predavanjih pogledali sistem dveh kubitov v stanju $\frac{1}{2} |00\rangle + \frac{1}{2} |10\rangle - \frac{1}{\sqrt{2}} |11\rangle$.

4 Kvantni algoritmi

Izpostavimo tri pomembnejše kvantne algoritme:

- Deutschov algoritem (prvi kvantni algoritem)
- Groverjev algoritem
- Shorov algoritem