

Elementi kvantnega računalništva

Bojan Golli

Pedagoška fakulteta, UL

predavanje

20. oktober 2022

Klasični računalniki

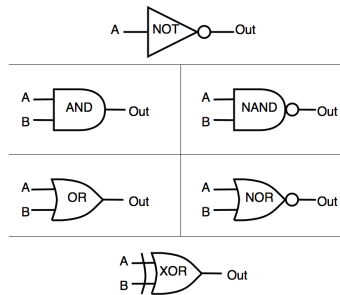
Osnovno enoto informacije predstavlja **bit** in lahko zavzame dve vrednosti, **0** in **1**. Bit realiziramo z enosmerno napetostjo, tako da bit **0** ustreza napetosti **0 V**, bit **1** pa napetosti **5 V** (ali nižji).

Kombinacije bitov **0011 1001** ... kodirajo kompleksnejšo informacijo: števila in črke.

Operacije nad biti izvajamo z elektronskimi vezji, ki jim pravimo logična vrata, na primer vrata AND, OR, NOT, NAND, NOR ...

Omejitve klasičnih računalnikov:

Večje zmogljivosti zahtevajo večje število tranzistorjev v čim manjši prostornini. Danes se velikosti tranzistorjev že približujejo velikosti atomov (**7 nm**). Pri manjših razdaljah bi lahko elektroni že nekontrolirano **tunelirali** skozi vezje in delovanje ne bi bilo več zanesljivo.



Kubit

Osnovna enota informacije v kvantnem računalniku je *kubit* (*qubit*).

Kubit je kvantno stanje, ki je linearna kombinacija dveh bazičnih kvantnih stanj, ki ju označimo z **0** in **1**:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle$$

a_0 in a_1 kompleksna koeficienta; stanje normirano: $|a_0|^2 + |a_1|^2 = 1$.

Interpretacija: $|a_0|^2$ ustreza *verjetnosti*, da je kubit v stanju $|0\rangle$, $|a_1|^2$ pa verjetnosti za stanje $|1\rangle$.

Kvantni stanji realiziramo na primer s **spinom elektrona**, katerega tretja komponenta lahko zavzame vrednost $-\frac{1}{2}\hbar$ in $\frac{1}{2}\hbar$, tako da $\frac{1}{2}\hbar$ ustreza **0**, $-\frac{1}{2}\hbar$ pa **1**.

Pri poskusih bolj pogosto uporabljajo dve spinski stanji **fotona** (levo in desno cirkularno polarizacijo).

Dve stanji lahko slikovito ponazorimo tudi z znaki $\uparrow$ — spin gor in $\downarrow$ — spin dol:

$$|\psi\rangle = a_0 \uparrow + a_1 \downarrow .$$

Fizikalna realizacija kubita

Kubit lahko realiziramo s katerikoli kvantnim sistemom, ki se lahko nahaja v **dveh stanjih**. Kubit lahko ustreza

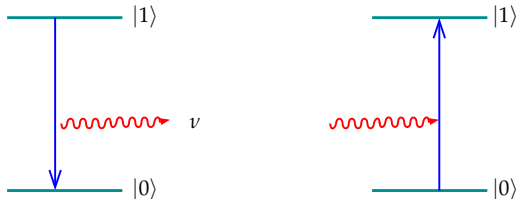
- elektronskemu spinu,
- jedrskemu spinu,
- dvema stanjem fotonske vrtilne količine (polarizaciji),
- osnovnemu in prvemu vzbujenemu stanju elektrona v atomu ali molekuli,
- stanjem Cooperjevih parov v Josephsonovem stiku,
- ujetimi ioni (trapped ions),
- kvantnim pikam ...

Zahtevamo pa:

- primerno dolga **obstočnost** stanj (nekaj sekund do 3 ur pri zelo nizki T .)
- koherenca: stanji sta **prepleteni**, tj. povezani v eno samo valovno funkcijo

Manipulacija kubitov

Kubite lahko orientiramo s pomočjo magnetnega ali električnega polja.



Pretvorbo (prehod) enega stanja v drugega lahko dosežemo s pomočjo elektromagnetnega valovanja.

Kubitni nizi

Podobno kot bite sestavimo več kubitov v niz.

V primeru 2 kubitov so 4 možne kombinacije 0 in 1: 00, 01, 10, 11.

$$|\Psi\rangle = a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle$$

Niz ustreza stanju — na primer — dveh fotonov;

$|a_0|^2$ predstavlja verjetnost, da je prvi foton v stanju $\uparrow$
in hkrati drugi foton tudi v $\uparrow$,

$|a_1|^2$ da je prvi v $\uparrow$ in drugi v $\downarrow \dots$

Podobno nizu treh kubitov ustreza stanje

$$|\Psi\rangle = a_0|000\rangle + a_1|001\rangle + a_2|010\rangle + a_3|011\rangle + a_4|100\rangle + a_5|101\rangle + a_6|110\rangle + a_7|111\rangle.$$

Procesiranje

Niz treh kubitov na začetku postopka postavimo na določeno vrednost, recimo $|000\rangle$, in procesiramo z zaporedjem *kvantnih vrat*.

Na koncu je niz lahko v katerem koli stanju $|000\rangle \dots |111\rangle$.

Ko na koncu postopka pomerimo spine delcev, dobimo izbrano stanje z verjetnostjo $|a_i|^2, i = 0, \dots, 7$.

Če poskus ponovimo, bomo v splošnem dobili drugačen rezultat.

Rezultat torej ni enoličen, s ponavljanem postopka lahko ugotovimo le verjetnosti za posamezne izide.

Kvantni računalniki torej niso primerni za reševanje vseh vrst problemov, ki jih sicer zastavljamo računalnikom, pač pa le za probleme, ki so prilagojeni stohastični naravi kubitov.

Programski jezik: *Qiskit*

Kvantna logična vrata

Klasična logična vrata nadomestijo **kvantna logična vrata**.

Operacije, s katerimi spreminjamo kubite, upodobimo z *unitarnimi* matrikami — to zagotavlja, da se norma kubita ohranja.

Značilne matrike:

Paulijeve matrike

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Hadamardova vrata

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

Obstajajo tudi vrata, ki delujejo nad dvemi in tremi kubitami (matrike 4×4 in 8×8)

Primeri operacij nad kubiti

Če kubit zapišimo v obliki

$$\uparrow = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \downarrow = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad a_0 \uparrow + a_1 \downarrow = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix},$$

velja

$$\sigma_x \downarrow = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \uparrow, \quad \sigma_x \uparrow = \downarrow,$$

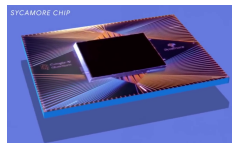
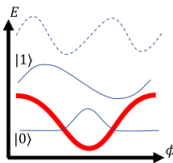
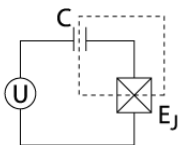
$$\sigma_x(a_0 \uparrow + a_1 \downarrow) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} a_1 \\ a_0 \end{bmatrix} = (a_1 \uparrow + a_0 \downarrow).$$

$$\sigma_z \uparrow = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \uparrow, \quad \sigma_z \downarrow = -\downarrow$$

$$\mathbf{H} \uparrow = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} (\uparrow + \downarrow),$$

Procesor Sycamore (Google)

53 kubitni procesor s **Cooperjevimi pari** v superprevodniku z **Josephsonovim stikom**. Stanje kubita 0 ustreza osnovno stanje para, stanju 1 pa prvo vzbujeno stanje, simbolično prikazanih na desni sliki.



https://commons.wikimedia.org/wiki/File:Google_Sycamore_Chip_002.png

Za stabilno delovanje procesorja je pomembno, da je energija nivojev bistveno nižja od vezavne energije elektronov v Cooperjevem paru; prav tako je bistveno, da je temperatura okolice dovolj nizka. Velja:
 vezavna energija para elektronov $E_J \approx 40 \text{ meV}$,
 razlika energij $E_1 - E_0 = 20 \text{ } \mu\text{eV}$, $\nu = 5 \text{ GHz}$.
 temperatura $T \approx 20 \text{ mK}$, $k_B T \approx 2 \text{ } \mu\text{eV}$.

Trenutno največji: IBM Eagle, 127 kubitov; Jiuzhang 2.0, (113 fotonov)

IBM-ov program razvoja

Development Roadmap | Executed by IBM On target

2019 Run quantum circuits
on the IBM cloud2020 Demonstrate and
prototype quantum
algorithms and
applications2021 Run quantum
programs 100x faster
with Qiskit Runtime

2022

Bring dynamic circuits to
unlock more computations

2023

Enhancing applications
with elastic computing
and parallelization of
Qiskit Runtime

2024

Improve accuracy of
Qiskit Runtime with
scalable error mitigation

2025

Scale quantum a
ctions with circuit
toolbox controls
Qiskit RuntimeModel
Developers

Prototype quantum software applications



Quantum softwa

Machine learning

Algorithm
DevelopersQuantum algorithm and application modules 

Machine learning | Natural science | Optimization

Quantum Serverless

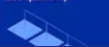
Intelligent orchestration

Circuit Knitting T

Kernel
DevelopersCircuits Qiskit Runtime Dynamic circuits 

Threaded primitives

Error suppression and mitigation

System
ModularityFalcon
27 qubits Hummingbird
65 qubits Eagle
127 qubits Osprey
433 qubits Condor
1,121 qubitsFlamingo
1,386+ qubitsKookaburra
4,158+ qubitsHeron
133 qubits x pCrossbill
408 qubits

Uporaba

- Kriptografija

$$M = P_1 P_2, \quad P_1, P_2 \text{ veliki praštevili}$$

Število M potuje po povezavi: sprejemnik pozna P_1 in izračuna

$$P_2 = \frac{M}{P_1}, \quad P_2 \dots \text{ključ za dekodiranje sporočila}$$

Če morebitni prisluškovalec ulovi število M , lahko le s poskušanjem ugotovi števili P_1 in P_2 .

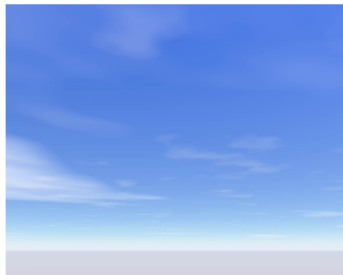
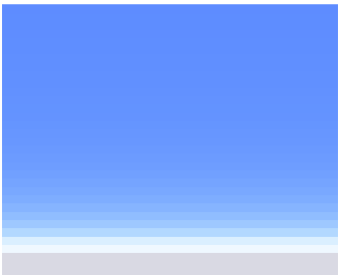
Danes verjamemo, da bo mogoče kodo razbijati s uporabo kvantnih računalnikov, zato ni čudno, da se za njihov razvoj zelo zanima in ga finančno podpira vojska.

Shorov algoritem na kvantnih računalnikih naj bi razbil kodo v doglednem času že na procesorju s petimi kubiti.

Danes pa že obstajajo algoritmi, ki so „odporni“ tudi na kvantne algoritme.

Uporaba

- **Kvantne simulacije:** struktura sistemov v mikroskopskem svetu, velike molekule, ...
- **NP polni problemi:** Optimalno rešitev najdemo le s poskušanjem vseh možnosti; zadovoljimo se tudi z dovolj optimalno rešitvijo (simulated annealing).
- **Metoda Monte Carlo:** že v klasični izvedbi ima probabilističen značaj, primer: Eva Markelj (diplomsko delo) *Računalniška simulacija sipanja svetlobe v atmosferi*



Kvantna prepletenost

Valovna funkcija dveh *nerazločljivih delcev* s spinom:

$$\Psi_{12}^{\pm} = \frac{1}{\sqrt{2}} (\uparrow_1 \downarrow_2 \pm \uparrow_2 \downarrow_1).$$

$$\Phi_{12}^{\pm} = \frac{1}{\sqrt{2}} (\uparrow_1 \uparrow_2 \pm \downarrow_2 \downarrow_1).$$

Prvi delec je z verjetnostjo 50% v stanju $\uparrow$ in s 50% verjetnostjo v stanju $\downarrow$; enako velja za drugi delec.

Ko pa naredimo poskus in izmerimo stanje prvega delca, je stanje drugega delca enolično določeno. (Če je prvi delec po meritvi v stanju $\uparrow$, je drugi delec v stanju $\downarrow$.)

Pravimo, da sta delca *prepletena*.

Po opravljeni meritvi pa delca delca nista več prepletena; pravimo, da je valovna funkcija razpadla ali *kolapsirala*.

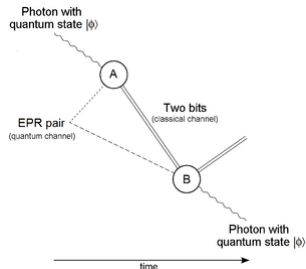
Letos (2022) so Nobelovo nagrado za fiziko prejeli Alain Aspect, John F. Clauser in Anton Zeilinger za poskuse s prepletenimi fotoni.

Teleportacija

V najbolj enostavnem primeru prenesemo en kubit informacije iz kraja A v kraj B.

$$\psi_C = \alpha \uparrow_C + \beta \downarrow_C.$$

Hkrati ustvarimo eno od štirih bazičnih stanj $\Psi^\pm, \Phi^\pm$ dveh delcev, označimo ju z A in B, recimo, da je to Ψ_{AB}^+ in jo prepletemo z delcem C. Delec B pošljemo v kraj B.



$$\begin{aligned}\Psi_{AB}^+ \cdot \psi_C &= \frac{1}{\sqrt{2}} (\alpha \uparrow_A \downarrow_B \uparrow_C + \beta \uparrow_A \downarrow_B \downarrow_C + \alpha \downarrow_A \uparrow_B \uparrow_C + \beta \downarrow_A \uparrow_B \downarrow_C) \\ &= \frac{1}{\sqrt{2}} (\alpha \uparrow_A \uparrow_C \downarrow_B + \beta \uparrow_A \downarrow_C \downarrow_B + \alpha \downarrow_A \uparrow_C \uparrow_B + \beta \downarrow_A \downarrow_C \uparrow_B).\end{aligned}$$

$$\Psi_{AC}^+ = \frac{1}{\sqrt{2}} (\uparrow_A \downarrow_C + \downarrow_A \uparrow_C), \quad \Psi_{AC}^- = \frac{1}{\sqrt{2}} (\uparrow_A \downarrow_C - \downarrow_A \uparrow_C),$$

$$\Phi_{AC}^+ = \frac{1}{\sqrt{2}} (\uparrow_A \uparrow_C + \downarrow_A \downarrow_C), \quad \Phi_{AC}^- = \frac{1}{\sqrt{2}} (\uparrow_A \uparrow_C - \downarrow_A \downarrow_C).$$

$$\uparrow_A \downarrow_C = \frac{1}{\sqrt{2}} (\Psi_{AC}^+ + \Psi_{AC}^-), \quad \downarrow_A \uparrow_C = \frac{1}{\sqrt{2}} (\Psi_{AC}^+ - \Psi_{AC}^-),$$

$$\uparrow_A \uparrow_C = \frac{1}{\sqrt{2}} (\Phi_{AC}^+ + \Phi_{AC}^-), \quad \downarrow_A \downarrow_C = \frac{1}{\sqrt{2}} (\Phi_{AC}^+ - \Phi_{AC}^-).$$

Teleportacija

Koeficienta α in β , ki vsebujeta informacijo o kubit, se sedaj pojavita v stanju delca B .

$$\begin{aligned}\Psi_{AB}^+ \cdot \psi_C &= \frac{1}{2} \Psi_{AC}^+ \cdot (\alpha \uparrow_B + \beta \downarrow_B) \\ &+ \frac{1}{2} \Psi_{AC}^- \cdot (\alpha \uparrow_B - \beta \downarrow_B) \\ &+ \frac{1}{2} \Phi_{AC}^+ \cdot (\alpha \downarrow_B + \beta \uparrow_B) \\ &+ \frac{1}{2} \Phi_{AC}^- \cdot (\alpha \downarrow_B - \beta \uparrow_B) .\end{aligned}$$

Stanje delca B je prepleteno s stanji delcev A in C , ki ostaneta pri v kraju A . Eksperimentator izmeri stanje delcev A in C . Pri meritvi dobi eno od štirih možnih stanj Ψ_{AC}^+ , Ψ_{AC}^- , Φ_{AC}^+ , ali Φ_{AC}^- . V tistem trenutku valovna funkcija treh delcev *kolapsira* in delec B se znajde v enem od štirih možnih kombinacij. Eksperimentator A pošlje Bju informacijo o svoji meritvi: če izmeri stanje

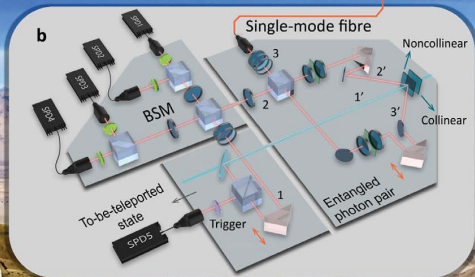
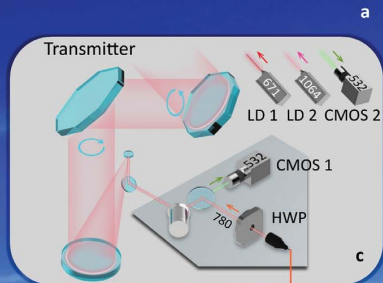
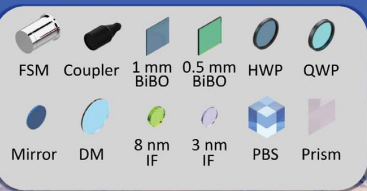
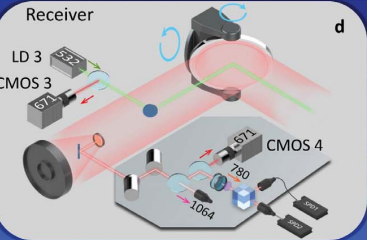
Ψ_{AC}^+ B je že v pravem stanju

Ψ_{AC}^- spremeni predznak pri spinu $\downarrow$ z uporabo vrat σ_z

Φ_{AC}^+ obrne orientaciji obeh spinov s σ_x

Φ_{AC}^- obrne orientaciji in spremeni predznak pri spinu $\uparrow$ z uporabo uporabo vrat σ_z in σ_x

Implementacija



Literatura

- Quantum computing, (16. 10. 2022), pridobljeno s https://en.wikipedia.org/wiki/Quantum_computing
- Qubit, (16. 10. 2022), pridobljeno s <https://en.wikipedia.org/wiki/Qubit>
- Quantum gate, (16. 10. 2022), pridobljeno s https://en.wikipedia.org/wiki/Quantum_gate
- B. Golli, Osnove moderne fizike, poglavje 9.
- Eva Markelj, Računalniško simuliranje sipanja svetlobe v atmosferi, Diplomsko delo, PeF, Ljubljana 2016, <http://pefprints.pef.uni-lj.si/3880/>
- Quantum entanglement, (16. 10. 2022), pridobljeno s https://en.wikipedia.org/wiki/Quantum_entanglement
- Quantum teleportation, (16. 10. 2022), pridobljeno s https://en.wikipedia.org/wiki/Quantum_teleportation
- Quantum Computers Explained – Limits of Human Technology <https://www.youtube.com/watch?v=JhHMCUmq28>