Kvantno računalo

Kvantna računala (SI)

5. prosinca 2019.

Prikaz stanja sustava klasičnih bitova

Stanja klasičnog bita možemo prikazati vektor-stupcima

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

Stanja sustava dvaju klasičnih bitova prikazujemo s

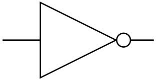
$$00 \leftrightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad \dots \qquad 11 \leftrightarrow \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Sustav n klasičnih bitova ili n-bitno klasično računalo može se naći u 2^n različitih stanja koja prikazujemo s 2^n linearno neovisnih vektor-stupaca dimenzije 2^n.

Nereverzibilnost klasičnog logičkog kruga

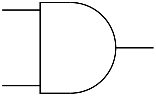
Klasična logička vrata prikazujemo simbolima i matricama:

NOT: x



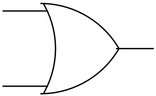
$\neg x$ $\quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

AND: x, y



$x \wedge y$ $\quad \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

OR: x, y

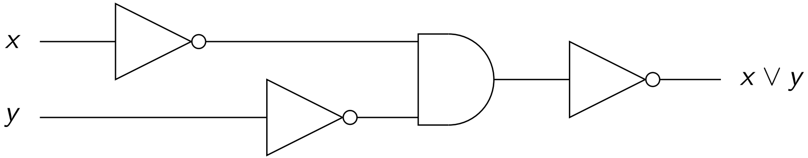


$x \vee y$ $\quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$

Složenija klasična vrata (klasični logički krug, klasično računalo) prikazujemo kao sekvencijalne sklopove jednostavnih logičkih vrata. Za tvorbu proizvoljno složenih vrata dovoljna su NOT i AND vrata (ili samo NAND vrata).

Primjer: Tvorba OR s pomoću NOT i AND

DeMorganov identitet: $x \vee y = \neg(\neg x \wedge \neg y)$



Matrični prikaz: $\mathrm{OR} = \mathrm{NOT} \cdot \mathrm{AND} \cdot (I \otimes \mathrm{NOT}) \cdot (\mathrm{NOT} \otimes I)$

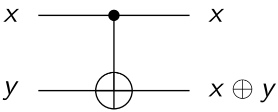
Općenito, na osnovi poznatog stanja na izlazu iz klasičnih vrata nije moguće rekonstruirati stanje na ulazu te kažemo da *klasična logička vrata općenito nisu reverzibilna*. Primjer reverzibilnih vrata su NOT vrata, dok nijedna vrata s većim brojem ulaznih od broja izlaznih bitova (AND, OR) nisu reverzibilna. Slijedi da u klasičnom logičkom krugu dolazi do

- gubitka informacije,
- povećanja entropije,
- utoška energije,
- te do oslobađanja topline (vidi Landauerov princip).

Također slijedi da se općeniti klasični logički krug *ne* ponaša u skladu s principom kvantne mehanike prema kojem je evolucija stanja sustava unitarna odn. reverzibilna.

cNOT, Toffolijeva i Fredkinova reverzibilna vrata

Upravljana NOT, control-NOT ili cNOT vrata (operator):



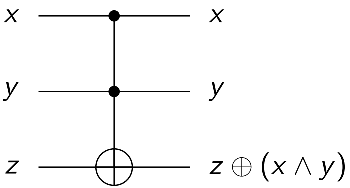
$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & & 1 \\ & & 1 & \end{pmatrix}$$

Bit x ima ulogu upravljačkog ili kontrolnog bita.

Operator $\oplus$ je binarni XOR operator odn. zbrajanje modulo 2.

Reverzibilnost: $\text{cNOT} \cdot \text{cNOT} = I$

Toffolijeva vrata (operator):



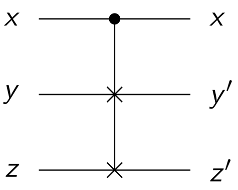
$$\begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & & 1 \\ & & & & & & 1 & \end{pmatrix}$$

Bitovi x i y su kontrolni bitovi.

Reverzibilnost: Toffoli $\cdot$ Toffoli $= I$

Univerzalnost: možemo konstruirati NOT i AND vrata

Fredkinova vrata (operator):



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

Bit x je kontrolni bit:

$$(0, y, z) \rightarrow (0, y, z) \qquad (1, y, z) \rightarrow (1, z, y)$$

Reverzibilnost: Fredkin $\cdot$ Fredkin $= I$

Univerzalnost: možemo konstruirati NOT i AND vrata

$$(x, 1, 0) \rightarrow (x, \neg x, x) \qquad (x, 0, z) \rightarrow (x, x \wedge z, (\neg x) \wedge z)$$

Postojanje univerzalnih reverzibilnih vrata (Toffolijeva ili Fredkinova vrata) implicira da je svaki klasični algoritam moguće izvesti korištenjem reverzibilnog logičkog kruga.

Reverzibilnost kvantnog logičkog kruga

Klasično računalo je sustav klasičnih bitova. n-bitno klasično računalo se može naći u 2^n različitih stanja.

Kvantno računalo je sustav kvantnih bitova (qubitova). Stanje n-qubitnog kvantnog računala je bilo koja linearna superpozicija 2^n stanja koja odgovaraju vektorima baze Hilbertovog prostora $\mathcal{H}^{\otimes n}$ dimenzije 2^n. Stanja koja odgovaraju vektorima baze možemo obilježiti s $|0\rangle, \ldots, |2^n - 1\rangle$.

Primjer: Vektori tzv. računalne baze 3-qubitnog računala su

$$|0\rangle = |000\rangle\,, \quad |1\rangle = |001\rangle\,, \quad |2\rangle = |010\rangle\,, \quad \ldots \quad |7\rangle = |111\rangle\,,$$

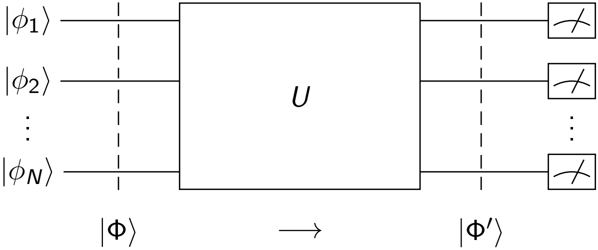
gdje je npr. $|5\rangle = |101\rangle = |1 \otimes 0 \otimes 1\rangle = |1\rangle \otimes |0\rangle \otimes |1\rangle$

Važno je uočiti sljedeću razliku između n-bitnog klasičnog i n-qubitnog kvantnog računala:

- Klasično računalo se može naći u 2^n različitih stanja. Pri mjerenju (očitanju) stanja ono ostaje nepromijenjeno.
- Kvantno računalo se može nalaziti u beskonačnom mnoštvu različitih stanja (linearne superpozicije 2^n stanja računalne baze). Mjerenjem (očitanjem) stanja kvantnog računala dobivamo neko od 2^n stanja računalne baze, nakon čega smatramo da računalo prelazi upravo u to stanje. To znači da je mjerenje (očitanje) stanja moguće obaviti samo jednom.

Evoluciju stanja kvantnog računala opisujemo unitarnom transformacijom

$$|\Phi\rangle \to |\Phi'\rangle = U\,|\Phi\rangle$$



Unitarnost transformacije podrazumijeva postojanje inverzne transformacije, $U^{-1} = U^{\dagger}$, odnosno *reverzibilnost računalnog postupka* koji računalo provodi.

S obzirom da je svaki klasični algoritam moguće formulirati s pomoću klasičnih reverzibilnih logičkih vrata, slijedi da je svaki klasični algoritam, barem u načelu, moguće izvesti i na kvantnom računalu.

Osim klasičnih algoritama, kvantna računala mogu izvoditi i tzv. kvantne algoritme koji se suštinski razlikuju od klasičnih algoritama.

Kvantna vrata (operatori) koji djeluju na jedan qubit

Vratima u kvantnom logičkom krugu smatramo bilo koji unitarni operator koji djeluje na jedan ili više qubitova.

Vrata odn. unitarni operator U koji djeluje na jedan qubit prikazujemo simbolom

$$—\boxed{U}—$$

Vrata su definirana relacijama

$$U|0\rangle = \alpha_{00}|0\rangle + \alpha_{10}|1\rangle$$
$$U|1\rangle = \alpha_{01}|0\rangle + \alpha_{11}|1\rangle$$

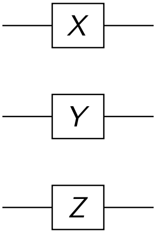
pri čemu je matrica $U = \begin{pmatrix} \alpha_{00} & \alpha_{01} \\ \alpha_{10} & \alpha_{11} \end{pmatrix}$ unitarna ($U^\dagger \cdot U = I$).

Primjer: Paulijeve matrice su unitarne te ih možemo koristiti kao kvantna vrata

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

$$\sigma_y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}$$

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



U prikazu stanja qubita na Blochovoj sferi, djelovanje operatora σ_x na općenito stanje qubita odgovara rotaciji stanja za kut π oko x-osi te vrijedi $\sigma_x^2 = I$. Analogno vrijedi za σ_y i σ_z.

Prepoznajemo $\sigma_x = \mathrm{NOT}$.

Primjer: Hadamardova vrata (operator)

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \text{—}\boxed{H}\text{—}$$

H pretvara stanja baze $\{|0\rangle, |1\rangle\}$ u stanja komplementarne baze $\{|+\rangle, |-\rangle\}$, gdje su $|\pm\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle \pm |1\rangle\big)$,

$$H|0\rangle = |+\rangle, \qquad H|1\rangle = |-\rangle.$$

H je vlastiti inverz: $H^\dagger \cdot H = H^2 = I$.

H možemo izraziti s pomoću Paulijevih matrica: $H = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z)$

Primjer: Vrata "korijen iz NOT" (square-root-of-NOT)

$$\sqrt{\mathrm{NOT}} = \sqrt{\sigma_x} = \frac{1}{1+\mathrm{i}} \begin{pmatrix} 1 & \mathrm{i} \\ \mathrm{i} & 1 \end{pmatrix}$$

Matrica je unitarna,

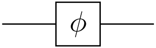
$$(\sqrt{\sigma_x})^\dagger \cdot \sqrt{\sigma_x} = I,$$

a vrata su dobila ime zbog svojstva

$$\sqrt{\sigma_x} \cdot \sqrt{\sigma_x} = \sigma_x.$$

Primjer: Operator faznog pomaka

$$R[\phi] = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\phi} \end{pmatrix}$$



U prikazu stanja na Blocohovoj sferi, operator $R[\phi]$ provodi rotaciju stanja oko z-osi za kut ϕ. Posebni slučajevi su

$$S = R[\pi/2] = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{pmatrix} \qquad \text{i} \qquad T = R[\pi/4] = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\pi/4} \end{pmatrix}$$

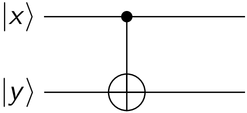
te Paulijev operator $\sigma_z = R[\pi]$.

Kvantna vrata cNOT i cU

Općenita kvantna logička vrata u $\mathcal{H}^{\otimes n}$ opisujemo unitarnom matricom dimenzije $2^n \times 2^n$.

Teorem (ovdje bez dokaza): Općenitu unitarnu transformaciju u $\mathcal{H}^{\otimes n}$ moguće je prikazati kao produkt cNOT vratiju i unitarnih transformacija nad pojedinačnim qubitovima.

Vrata cNOT preuzimamo iz klasične logike:



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

Ako se stanja $|x\rangle$ i $|y\rangle$ qubitova na ulazu u vrata cNOT podudaraju s vektorima računalne baze $\{|0\rangle, |1\rangle\}$, djelovanje kvantnih logičkih vratiju cNOT možemo izraziti kao

$$|x\rangle \otimes |y\rangle \to |x\rangle \otimes |x \oplus y\rangle .$$

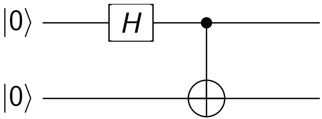
Koristeći stanja računalne baze 2-qubitnog računala imamo

$$|00\rangle \to |00\rangle , \quad |01\rangle \to |01\rangle , \quad |10\rangle \to |11\rangle , \quad |11\rangle \to |10\rangle .$$

Primjer: Neka se sustav dvaju qubitova početno nalazi u stanju

$$|\Phi\rangle = |0\rangle \otimes |0\rangle = |00\rangle \, .$$

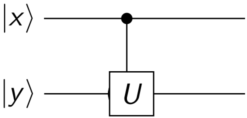
Na izlazu iz logičkog kruga



dobivamo spregnuto stanje

$$|\Phi'\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle \big).$$

Operator cU (control-U), gdje je U unitarni operator koji djeluje na stanje jednog qubita, možemo shvatiti kao poopćenje operatora cNOT:



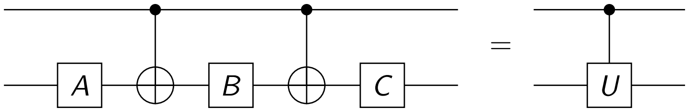
$$\begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$$

Qubit $|x\rangle$ je kontrolni qubit, a $|y\rangle$ je ciljni qubit:

- Ako $|x\rangle = |0\rangle$ onda $|y\rangle$ ostaje nepromijenjen.
- Ako $|x\rangle = |1\rangle$ onda $|y\rangle \to U\,|y\rangle$.

Odabirom $U = \sigma_x =$ NOT dobivamo operator cNOT.

Primjer: Operator cU možemo konstruirati s pomoću kruga



ako unitarni operatori A, B i C zadovoljavaju uvjete

$$CBA = I, \qquad C\sigma_x B\sigma_x A = U.$$

Blok-matrični prikaz:

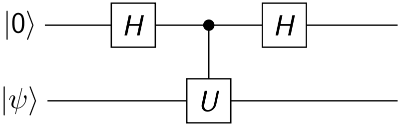
$$\begin{pmatrix} C & 0 \\ 0 & C \end{pmatrix} \cdot \begin{pmatrix} I & 0 \\ 0 & \sigma_x \end{pmatrix} \cdot \begin{pmatrix} B & 0 \\ 0 & B \end{pmatrix} \cdot \begin{pmatrix} I & 0 \\ 0 & \sigma_x \end{pmatrix} \cdot \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$$

$$= \begin{pmatrix} CBA & 0 \\ 0 & C\sigma_x B\sigma_x A \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$$

Primjer: Neka je $|\psi\rangle$ svojstveno stanje unitarnog operatora U sa svojstvenom vrijednošću λ,

$$U|\psi\rangle = \lambda|\psi\rangle, \qquad |\lambda| = 1.$$

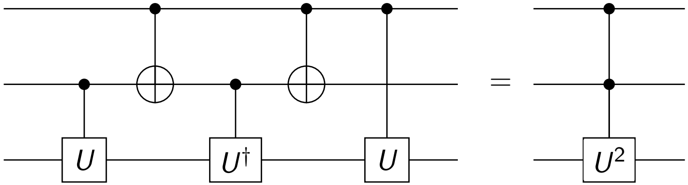
Na izlazu iz logičkog kruga



dobivamo stanje

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

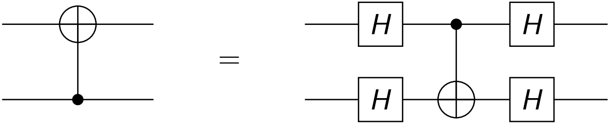
Primjer: Ako je U unitarni operator, vrijedi sljedeći identitet među kvantnim logičkim krugovima:



Toffolijeva vrata dobivamo uz odabir

$$U = \sqrt{\sigma_x} = \frac{1}{1+\mathrm{i}} \begin{pmatrix} 1 & \mathrm{i} \\ \mathrm{i} & 1 \end{pmatrix}.$$

Primjer: Preokrenuta cNOT vrata



Primjer: Realizacija SWAP operatora cNOT vratima