Kvantno računalo

Kvantna računala (SI)

13. siječnja 2017.

Stanje računala i prikaz broja

Klasično računalo koristi klasične bitove. N-bitno klasično računalo se može naći u nekom od 2^N različitih stanja koja možemo shvatiti kao prikaz brojeva $0, 1, \ldots, 2^N - 1$.

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 $\mathcal{H}^{\otimes N}$. Stanja koja odgovaraju vektorima baze možemo obilježiti s $|0\rangle, \ldots, |2^N - 1\rangle$.

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

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

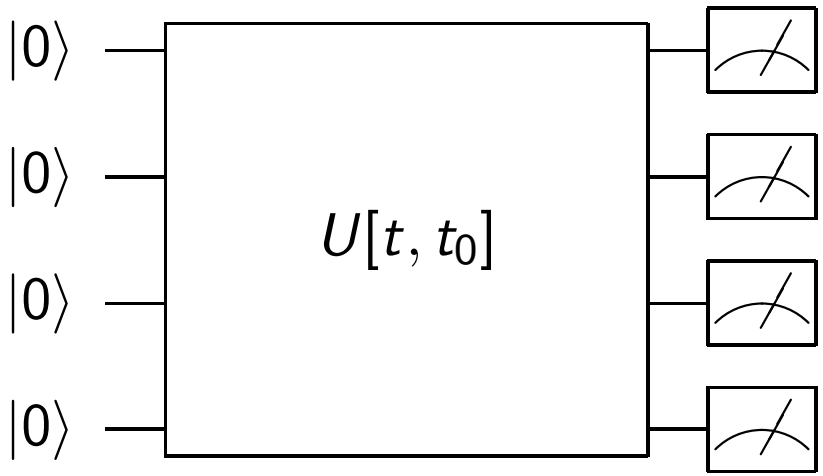
gdje je npr. $|5\rangle = |101\rangle = |1 \otimes 0 \otimes 1\rangle = |1\rangle \otimes |0\rangle \otimes |1\rangle$

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

- Klasično računalo se može naći u 2^N različitih stanja. Mjerenjem (očitanjem) stanja računala, njegovo stanje ostaje nepromijenjeno.
- Kvantno računalo se može nalaziti u beskonačnom mnoštvu različitih stanja (linearne superpozicije 2^N stanja računalne baze). Mjerenjem stanja kvantnog računala dobivamo neko od 2^N stanja računalne baze, a samo računalo prelazi upravo u to stanje. To znači da mjerenjem mijenjamo stanje kvantnog računala.

Reverzibilnost kvantnog računala

Ako je računalo dovoljno dobro izolirano od utjecaja okoline, vremensku evoluciju stanja računala možemo opisati unitarnom transformacijom.



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

Klasični algoritam na kvantnom računalu

Svaka klasična logička vrata možemo implementirati korištenjem tzv. not-AND (NAND) vratiju,

$$(x, y) \rightarrow 1 \oplus xy,$$

koja su nereverzibilna samim time što na izlazu imaju manji broj bitova od broja bitova na ulazu.

Klasični računalni algoritam je općenito nereverzibilan jer koristi nereverzibilna logička vrata.

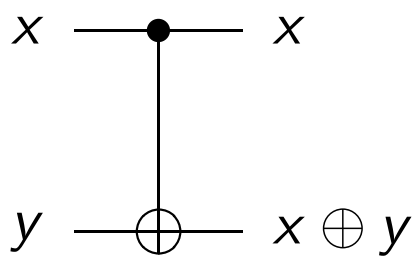
S obzirom da je kvantno računalo reverzibilno, klasični algoritam koji želimo izvoditi na kvantnom računalu moramo formulirati korištenjem isključivo reverzibilnih logičkih vrata.

cNOT (control-NOT) reverzibilna vrata:

$$(x, y) \to (x, x \oplus y)$$

Bit x zovemo kontrolnim bitom, a bit y zovemo ciljnim bitom.

cNOT vrata prikazujemo simbolom:



Reverzibilnost cNOT vratiju očituje se iz "tablice":

$$(00) \to (00), \quad (01) \to (01), \quad (10) \to (11), \quad (11) \to (10)$$

cNOT vrata omogućuju implementaciju linearne funkcije

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} \lambda \\ \mu \end{pmatrix}$$

gdje su $\alpha, \ldots, \mu$ numerički koeficijenti, ali ne i općenite reverzibilne funkcije.

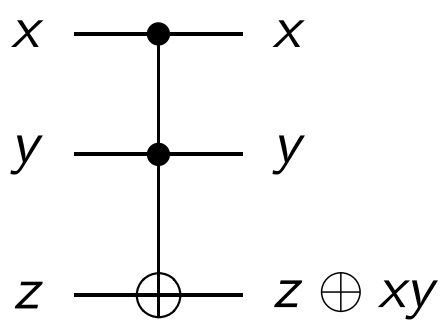
Implementacija općenite reverzibilne funkcije moguća je primjenom univerzalnih reverzibilnoih vratiju poznatih kao Toffolijeva vrata...

Toffolijeva reverzibilna vrata:

$$(x, y, z) \rightarrow (x, y, z \oplus xy)$$

Bitovi x i y su kontrolni bitovi, a z je ciljni bit.

Toffolijeva vrata prikazujemo simbolom:



Uočavamo da Toffolijeva vrata uz $z = 1$ izvode operaciju NAND na reverzibilan način.

Kvantna logička vrata kao unitarni operator u $\mathcal{H}^{\otimes n}$

Općenita vremenska evolucija koja se odvija u n-qubitnom kvantnom računalu jest unitarna transformacija u 2^n-dimenzionalnom Hilbertovom prostoru $\mathcal{H}^{\otimes n}$.

Općenita 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.

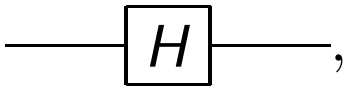
Hadamardova vrata

Hadamardova vrata odn. operator H djeluje na jedan qubit pretvarajući stanja baze $\{|0\rangle, |1\rangle\}$ u stanja komplementarne baze $\{|+\rangle, |-\rangle\}$ definirana s

$$H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big), \quad H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big).$$

Svojstvo $H^2 = I$ pokazuje da je H unitaran.

Hadamardova vrata u logičkom krugu prikazujemo simbolom

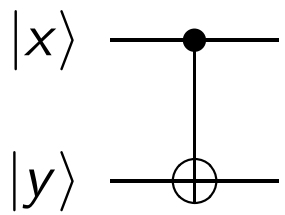


a Matrični prikaz Hadamardovog operatora u $\mathcal{H}^2$ je:

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

Vrata cNOT i cU

U kvantnom logičkom krugu vrata cNOT prikazujemo simbolom



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

$$|x\rangle \otimes |y\rangle \rightarrow |x\rangle \otimes |x \oplus y\rangle ,$$

odnosno koristeći stanja računalne baze 2-qubitnog računala imamo

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

Matrični prikaz vratiju cNOT u računalnoj bazi je

$$\text{cNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & \sigma_x \end{pmatrix},$$

gdje je σ_x Paulijeva matrica.

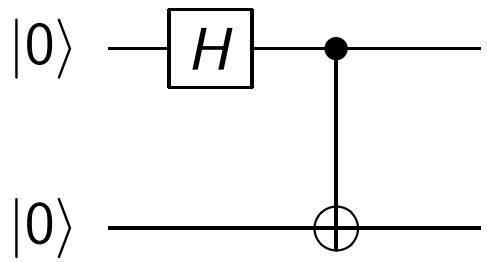
Uočavamo svojstvo $(\text{cNOT})^2 = I$ koje potvrđuje svojstvo unitarnosti operatora cNOT.

Također uočavamo da operator cNOT nije moguće napisati kao tenzorski produkt dvaju operatora koji djeluju u Hilbertovim prostorima pojedinačnih qubitova.

Primjer. Neka se sustav dvaju qubitova početno nalazi u stanju

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

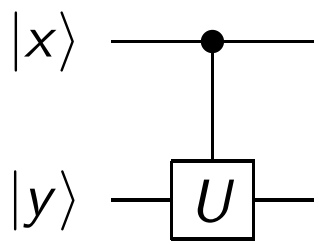
Na izlasku iz logičkog kruga



dobivamo spregnuto stanje

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

Ako je U unitarni operator koji djeluje na stanje jednog qubita, operator cU (control-U) možemo shvatiti kao poopćenje operatora cNOT. U kvantnom logičkom krugu prikazujemo ga simbolom



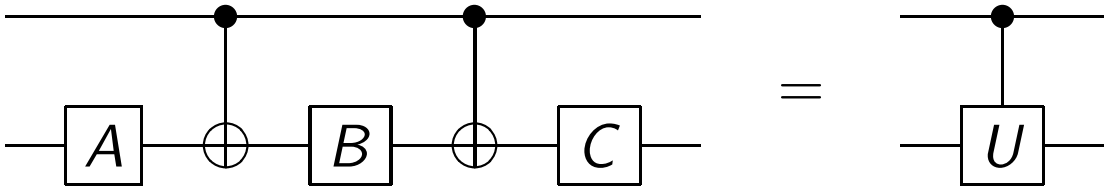
cU je unitarni operator sa svojstvima:

- $|x\rangle = |0\rangle$: stanje ciljnog qubita ostaje nepromijenjeno.
- $|x\rangle = |1\rangle$: stanje ciljnog qubita $|y\rangle \to U|y\rangle$.

Blok-matrični prikaz operatora cU je

$$\mathrm{cU} = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}.$$

Primjer. Operator cU možemo konstruirati s pomoću kruga



ako unitarni operatori A, B i C zadovoljavaju uvjete

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

koji slijede iz jednakosti blok-matričnih prikaza operatora:

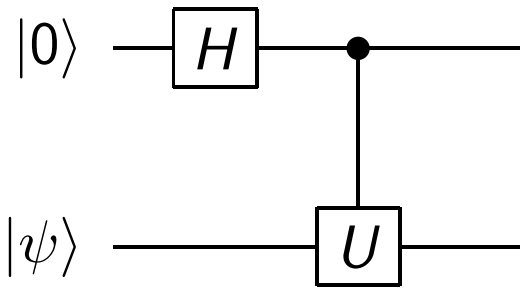
$$\begin{pmatrix} C & 0 \\ 0 & C \end{pmatrix} \cdot \begin{pmatrix} I & 0 \\ 0 & \sigma_x \end{pmatrix} \cdot \begin{pmatrix} B & 0 \\ 0 & B \end{pmatrix} \cdot \begin{pmatrix} I & 0 \\ 0 & \sigma_x \end{pmatrix} \cdot \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$$

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

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

$$U|\psi\rangle = \lambda|\psi\rangle .$$

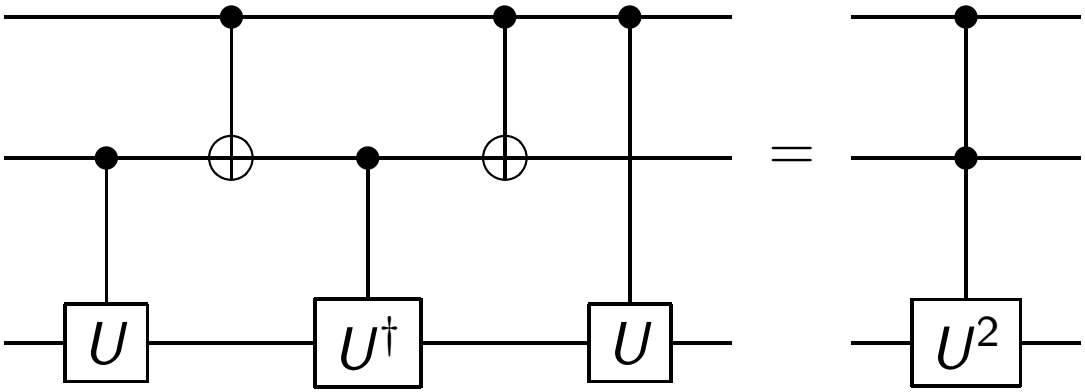
Na izlasku iz logičkog kruga



dobivamo stanje

$$\frac{1}{\sqrt{2}}\big(|0\rangle + \lambda|1\rangle\big) \otimes |\psi\rangle .$$

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



Toffolijeva vrata dobivamo uz odabir

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

Načelo kvantnog paralelizma

Početno stanje kvantnog računala ne mora biti neko od stanja računalne baze, već može biti bilo koja superpozicija tih stanja. Konačno stanje kvantnog računala tad je superpozicija stanja koja bismo dobili uz početna stanja jednaka stanjima računalne baze.

To znači da jedno jedino konačno stanje kvantnog računala može ovisiti o (kažemo sadržavati informaciju o) rezultatu koji bismo dobili uz sva moguća početna stanja.

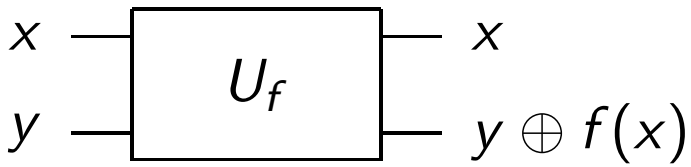
Mogućnost nekih kvantnih logičkih operacija (algoritama) da u jednom koraku obave račun nad više različitih vrijednosti svog argumenta zovemo *kvantnim paralelizmom*.

Važno je naglasiti da načela kvantne fizike ne dopuštaju da mjerenjem konačnih stanja qubitova kvantnog računala pristupimo svoj informaciji koja je prisutna u konačnom stanju računala.

U klasičnom računalu, funkciju $f : \{0,1\} \to \{0,1\}$ možemo implementirati kao unitarnu transformaciju U_f:

$$(x, y) \xrightarrow{U_f} (x, y \oplus f(x))$$

Prikazano simbolom:



Gornji bit zovemo ulaznim bitom, a donji bit zovemo izlaznim bitom.

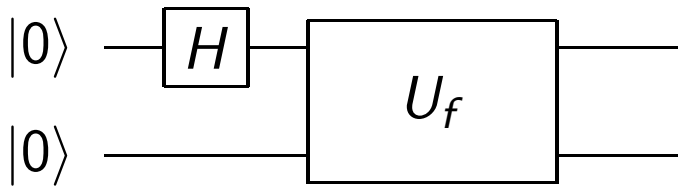
Reverzibilnost vrata odnosno unitarnost operatora slijedi iz svojstva $U_f^2 = I$:

$$(x, y) \xrightarrow{U_f^2} (x, (y \oplus f(x)) \oplus f(x)) = (x, y)$$

Kvantna vrata koja predstavljaju implementaciju funkcije $f : \{0,1\} \to \{0,1\}$, tzv. *quantum oracle*, imaju svojstvo

$$U_f \left|x \otimes y\right\rangle = \left|x \otimes (y \oplus f(x))\right\rangle, \qquad (x, y \in \{0,1\}).$$

Primjer. Na izlasku iz kvantnog kruga



stanje sustava je

$$\frac{1}{\sqrt{2}}\left(\left|0 \otimes f(0)\right\rangle + \left|1 \otimes f(1)\right\rangle \right).$$

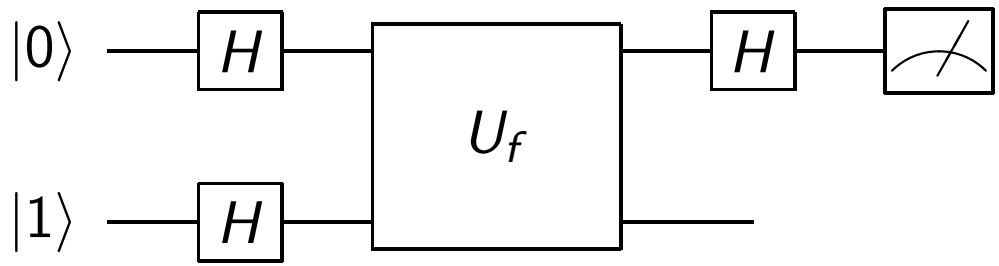
Uočavamo da konačno stanje ovisi o (sadrži informaciju o) vrijednostima funkcije u dvama različitim vrijednostima argumenta.

Deutschev algoritam

Cilj je odrediti je li funkcija $f : \{0,1\} \to \{0,1\}$ "uravnotežena", $f(1) \neq f(0)$, ili je "konstantna", $f(1) = f(0)$.

Koristeći kvantni paralelizam, Deutschev algoritam rješava postavljeni problem uz samo jednu evaluaciju vrata U_f odnosno bez da zasebno izračunamo vrijednosti $f(0)$ i $f(1)$ te ih usporedimo.

Kvantni logički krug Deutschevog algoritma je



gdje vrata U_f predstavljaju kvantnu implementaciju funkcije f.

Ulazni i izlazni registar pripremamo u stanjima $|0\rangle$ i $|1\rangle$.

Pokazuje se da konačno stanje ulaznog registra (gornjeg qubita) možemo izraziti kao

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

Uočavamo da uz konstantnu f dobivamo konačno stanje $|0\rangle$, dok za uravnoteženu f dobivamo stanje $|1\rangle$.

Uočavamo da mjerenjem stanja ulaznog registra (gornjeg qubita) možemo odrediti je li funkcija f konstantna ili je uravnotežena.

Analiza toka Deutschevog algoritma:

- Početna stanja qubitova su $|0\rangle$ i $|1\rangle$ što znači da je sustav u stanju
$$|0\rangle \otimes |1\rangle = |01\rangle .$$
- Nakon prolaska parom Hadamardovih vrata sustav je u stanju
$$H|0\rangle \otimes H|1\rangle = |+\rangle \otimes |-\rangle = |+-\rangle .$$
- Kratkim računom možemo pokazati da za $x \in \{0, 1\}$ vrijedi
$$U_f |x-\rangle = (-1)^{f(x)} |x-\rangle .$$

- Koristeći prethodni rezultat nalazimo stanje sustava po izlasku iz U_f

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

gdje uočavamo da se radi o nespregnutom stanju s ulaznim registrom u stanju opisanim vektorom

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

- Primjenom Hadamardovog operatora na stanje ulaznog registra po izlasku iz vrata U_f dobivamo konačno stanje

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

Poopćenje na n-ulaznih i m-izlaznih qubitova

- Ulazni registar koji sadrži argument funkcije $f(x)$ sastoji se od n-qubitova čija stanja prikazujemo bazom

$$\{|x\rangle ; x = 0, \ldots, 2^n - 1\},$$

gdje je $|x\rangle = |x_{n-1} \ldots x_1 x_0\rangle$, a $x_{n-1}, \ldots, x_1, x_0$ poprimaju vrijednosti 0 ili 1.

- Izlazni registar se sastoji od m-qubitova koliko je potrebno da se prikaže funkcijsku vrijednost. Koristimo bazu

$$\{|z\rangle ; z = 0, \ldots, 2^m - 1\},$$

gdje je $|z\rangle = |z_{m-1} \ldots z_1 z_0\rangle$, ...

- Hadamardov operator proširujemo na tenzorski produkt Hadamardovih operatora. Kad je riječ o ulaznom registru imamo

$$H^{\otimes n} |0^{\otimes n}\rangle = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle .$$

- Vrata U_f koja predstavljaju implementaciju funkcije $f(x)$ definiramo kao

$$U_f |x \otimes z\rangle = |x \otimes (z \oplus f(x))\rangle ,$$

gdje je $\oplus$ operacija zbrajanja mod-2 bez prijenosa (*bitwise*).

- Unitarnost U_f slijedi iz svojstva $U_f^2 = I$.

- Pokazuje se da vrijedi $U_f \left| x \otimes 0^{\otimes m} \right\rangle = \left| x \otimes f(x) \right\rangle$.
- Ulazni registar pripremamo u stanju $\left| 0^{\otimes n} \right\rangle$ te ga propuštamo kroz Hadamardova vrata. Izlazni registar pripremamo u stanju $\left| 0^{\otimes m} \right\rangle$. Na izlazu iz vrata U_f imamo stanje

$$U_f \left(\left(H^{\otimes n} \left| 0^{\otimes n} \right\rangle \right) \otimes \left| 0^{\otimes m} \right\rangle \right) = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} U_f \left| x \otimes 0^{\otimes m} \right\rangle$$
$$= \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} \left| x \otimes f(x) \right\rangle$$

koje u sebi sadrži informaciju o vrijednostima koje funkcija f poprima u svih 2^n različitih vrijednosti njenog argumenta.