Deutschev algoritam

Kvantna računala (SI)

15. prosinca 2020.

Načelo kvantnog paralelizma

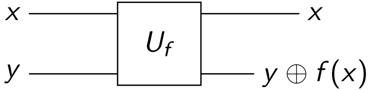
- Ako je početno stanje kvantnog računala superpozicija stanja računalne baze, onda je konačno stanje računala superpozicija odgovarajućih konačnih stanja.
- To znači da jedno jedino konačno stanje kvantnog računala može sadržavati informaciju o rezultatu koji bismo dobili za niz različitih početnih stanja.
- Mogućnost nekih kvantnih logičkih krugova (algoritama) da u jednom koraku obave račun nad više različitih vrijednosti svog argumenta zovemo *kvantnim paralelizmom*.

Funkcija jednog qubita

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, a donji bit izlaznim bitom.

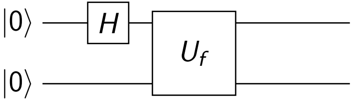
Reverzibilnost vrata odnosno unitarnost operatora slijedi iz svojstva $U_f^2 = I$:

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

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

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

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

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

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

  odn. $|x\rangle = |x_{n-1} \cdots x_1 x_0\rangle$ pri čemu $x_{n-1}, \ldots, x_1, x_0$ poprimaju vrijednosti 0 ili 1.

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

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

  odn. $|z\rangle = |z_{m-1} \cdots z_1 z_0\rangle$, ...

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

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

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

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

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

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

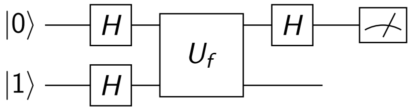
koje u sebi sadrži informaciju o vrijednostima koje funkcija f poprima u svih 2^n različitih vrijednosti njenog argumenta.

Osnovni oblik Deutschevog algoritma

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 tj. bez zasebnog izračuna i usporedbe vrijednosti $f(0)$ i $f(1)$.

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 $|1\rangle$.

To znači 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

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

što znači da se radi o separabilnom stanju s ulaznim registrom u stanju

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

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

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

Za konstantnu funkciju f qubit je u stanju $|0\rangle$, dok je za balansiranu f on u stanju $|1\rangle$.

To znači da mjerenjem konačnog stanja prvog qubita određujemo je li f konstantna ili balansirana uz samo jednu evaluaciju kvantne implementacije funkcije f.