ALGORITEM DEUTSCH - JOZSA

Dejan Arzenšek

20. maj 2008

Povzetek

Kvantni algoritem, ki sta ga predlagala David Deutsch in Richard Jozsa leta 1992, se imenuje Deutsch-Jozsa algoritem. Je eden prvih primerov kvantnih algoritmov, ki so bolj učinkoviti od vseh možnih klasičnih algoritmov.

1 ALGORITEM

V Deutsch-Jozsa problemu, imamo kvantno računalniško črno skrinjico (orakelj), ki realizira funkcijo $f : \{0,1\}^n \longrightarrow \{0,1\}$.

Obetamo si, da je funkcija ali *KONSTANTA* (0 na vseh vhodih ali 1 na vseh vhodih), ali *URAVNOTEŽENA* (vrne 1 za polovico vhodov ter 0 za drugo polovico). Torej z uporabo orakelja določimo, ali je f konstanta ali uravnotežena.

V konvencionalnem algoritmu potrebujemo $2^{n-1} + 1$ ovrednotenj za f, kjer je n število bitov. To je število odgovorov, ki da pravilno vrednost. Pri Deutsch-Josza kvantnemu algoritmu dobimo odgovor, ki je vedno pravilen le z enim samim ovrednotenjem f.

Definiramo funkcijo s številoma (kubitoma) $|0\rangle$ in $|1\rangle$). Z spodnjo tabelo so prikazani možni rezultati te funkcije.

	f_1	f_2	f_3	f_4
0	0	1	0	1
1	0	1	1	0
	$\overbrace{\qquad}^{}$ *konstanta*	$\overbrace{\quad}^{}$ *konst.*	$\overbrace{\quad}^{}$ *nekonst.*	$\overbrace{\quad}^{}$ *nekonst.*

Nekdo si je zamislil eno izmed teh štirih funkcij. Kolikokrat je treba poskušati, da vidimo, če je konstantna ali nekonstantna funkcija? Iz zgornjega primera vidimo, da je potrebno dvakrat ugibati.

Sedaj vzamemo za vhodno vrednost dve števili. Dobimo takšno tabelo:

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	....
00	0	1	1	1	0	0	1	0	
01	0	1	1	0	0	1	0	1	
10	0	1	0	1	1	0	0	1	.....
11	0	1	0	0	1	1	1	0	

V zgornjem primeru imamo zopet dve kontantni funkciji, 14 nekonstantnih, 6 uravnoteženih ter še 8, katere pa nas ne zanimajo. Tukaj se da s tremi poskusi ugotoviti ali je konstanta ali uravnotežena funkcija. Tako lahko nadaljujemo naprej z dodajanjem števil. Veljata te dve enačbi za število poskušanj, če je funkcija konstanta ali ne.

$$\frac{\text{št. kombinacij}}{2} + 1, \qquad \text{ali} \qquad 2^{n-1} + 1,$$

kjer je n število kubitov.

Poglejmo si sedaj kaj dobimo, če pošljemo v črno škatlo en vhod z vrednostjo $|x\rangle$, na drug vhod pa $|y\rangle$. Iz črne škatle pa imamo dva izhoda. Na zgornjem (nasproti vhodnemu $|x\rangle$), imamo zopet $|x\rangle$. Na spodnjem (nasproti vhodnemu $|y\rangle$), pa dobimo vrednost $|y \oplus f(x)\rangle$. $f(x)$ je ena izmed vrednosti $f_1, f_2, f_3, \ldots$. Operacija $\oplus$ pomeni seštevanje po modulu 2. To operacijo prikazujejo spodnje štiri vrstice:

$$\begin{array}{ccccc} 0 & \oplus & 0 & = & 0 \\ 0 & \oplus & 1 & = & 1 \\ 1 & \oplus & 0 & = & 1 \\ 1 & \oplus & 1 & = & 0 \end{array}$$

Torej ta operacija deluje tako, da ko seštejemo vrednosti in ta seštevek delimo z dva, pogledamo ostanek tega deljenja. Ta ostanek je potem izhodna vrednost te operacije.

Naredimo sedaj korak prehoda skozi črno škatlo za en kubit na vhodih. Torej je na vhodu $|x, y\rangle$, na izhodu pa $|x, y \oplus f(x)\rangle$. To naredim za vse štiri funkcije $f(x)$.

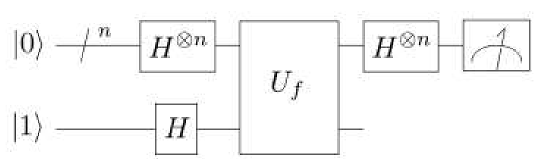
$\lvert x,y\rangle$	$\lvert x, y \oplus f_1(x)\rangle$	$\lvert x,y\rangle$	$\lvert x, y \oplus f_2(x)\rangle$	$\lvert x,y\rangle$	$\lvert x, y \oplus f_3(x)\rangle$	$\lvert x,y\rangle$	$\lvert x, y \oplus f_4(x)\rangle$
00	00	00	01	00	00	00	01
10	10	10	11	10	11	10	10
01	01	01	00	01	01	01	00
11	11	11	10	11	10	11	11

Za vsako od teh štirih vhodnih in izhodnih vrednosti lahko naredimo transformacijske matrike med vhodnimi in izhodnimi vrednostmi. Dobimo te štiri matrike:

$$\text{za } f_1 : \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ za } f_2\text{:} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ za } f_3\text{:} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ za } f_4\text{:} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Iz zgornjih matrik lahko opazim, da za f_1 ima obliko identične matrike, za f_2 nima kakšne posebne oblike. Za f_3 ima obliko operatorja CNOT, ki deluje na dva spina hkrati, za f_4 pa je operator CNOT, ki deluje na en spin.

V črni škatli je ena izmed štirih matrik. Mi bi radi z enim samim poskusom ugotovili za katero gre. Shematično lahko algoritem prikažemo z spodnjo sliko. Na zgornji sliki lahko vidimo,



Slika 1: Shematska slika algoritma.

da na dveh vhodih najprej delujemo z Hadamardovim operatorjem. Ta se zapiše kot:

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

Tako pretransformirana kubita vodimo naprej do črne škatle. Izhoda iz te črne škatle sta zopet dva. Zgornji vhod zopet pretransformiramo z Hadamardovo matriko. To pretransformirano vrednost pa na koncu izmerimo.

Torej, poglejmo kaj dobimo, če na zgornji vhod pošljemo $|0\rangle$, na spodnjega pa $|1\rangle$. $|0\rangle$ lahko zapišem vektorsko kot $[1, 0]$ ter $|1\rangle$ kot $[0, 1]$. Torej, če na ta dva kubita delujemo z operatorjem H, dobim na zgornjem vhodu vrednost $\frac{1}{\sqrt{2}}[1, 1]$ ter na spodnjem $\frac{1}{\sqrt{2}}[1, -1]$. Skupno funkcijo lahko tako zapišemo kot:

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

V vektorski obliki lahko to zapišem kot

$$\frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}$$

To funkcijo sedaj pošljem v črno škatlo in tako za vsako od štirih prej izračunanih matrik dobim ven te štiri vrednosti:

$$\text{za } f_1\text{:} \quad \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} \quad \text{za } f_2\text{:} \quad \frac{1}{2}\begin{pmatrix} -1 \\ 1 \\ -1 \\ 1 \end{pmatrix} \quad \text{za } f_3\text{:} \quad \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix} \quad \text{za } f_4\text{:} \quad \frac{1}{2}\begin{pmatrix} -1 \\ 1 \\ 1 \\ -1 \end{pmatrix}$$

Na koncu naredim še Hadamarda na prvi spin.
Hočem naredit Hadamardovo matriko na prvi spin. Napišem tele enačbe:

$$\begin{array}{lcl} H_1|00\rangle & \longrightarrow & \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle \\ H_1|01\rangle & \longrightarrow & \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle \\ H_1|10\rangle & \longrightarrow & \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|10\rangle \\ H_1|11\rangle & \longrightarrow & \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|11\rangle \end{array}$$

Iz teh enačb sledi operator H_1 kot matrika:

$$H_1 = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Delujmo sedaj z operatorjem H_1 na vrednost, ki jo dobimo ven iz črne škatlice za f_1:

$$H_1 \cdot \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} \quad = \quad \frac{1}{2\sqrt{2}}\begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}$$

Če poračunam še na preostalih treh funkcijah dobim spodnje vrednosti:

$$\text{za } f_2\text{:}\quad \frac{1}{2\sqrt{2}}\begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \qquad \text{za } f_3\text{:}\quad \frac{1}{2\sqrt{2}}\begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix} \qquad \text{za } f_4\text{:}\quad \frac{1}{2\sqrt{2}}\begin{pmatrix} 0 \\ 0 \\ -1 \\ 1 \end{pmatrix}$$

Tako pogledamo kakšne so vrednosti na samo prvem spinu!

Iz rezultatov se vidi, da pri meritvi prvega spina dobimo z gotovostjo $|0\rangle$ za obe konstantni funkciji in z gotovostjo $|1\rangle$ za obe uravnoteženi funkciji.

Algoritem torej loči konstantni funkciji od uravnoteženih z enim samim izračunom funkcije.