Deutschův algoritmus

Deutschův algoritmus je nejjednodušší příklad toho, že kvantové počítače jsou schopny výpočtů, které přesahují schopnosti počítačů klasických. Předpokládejme, že je dána funkce $f : \{0,1\} \mapsto \{0,1\}$ pomocí nějakého orákula (neboli „černé skříňky“, která na vstupu x vrací hodnotu $f(x)$, aniž bychom cokoli věděli o způsobu výpočtu této hodnoty). Úkolem je rozhodnout, zda je f konstantní, nebo ne. V klasickém případě je zřejmé, že musíme provést dva dotazy, tedy zjistit obě hodnoty funkce f. Na druhou stranu si všimněme, že otázka směřuje na jediný bit informace: „konstantní ano, nebo ne“? Neexistuje však žádný způsob, jak takovou otázku orákulu položit. To je přesně bod, ve kterém má kvantový počítač převahu.

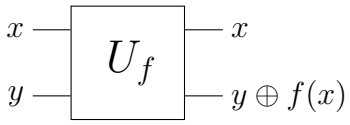
Situace se poněkud komplikuje otázkou, jak má vypadat kvantové orákulum. Z postulátů kvantové mechaniky plyne, že by to měla být nějaká unitární transformace. Problém je ovšem v tom, že funkce f nemusí být injektivní, tedy ani regulární, tím méně unitární. Standardní řešení tohoto problému spočívá v zavedení pomocného kubitu, který reprezentuje vstupní hodnotu. Funkce f bude tedy odpovídat dvoukubitovému operátoru U_f, který je pro $x, y \in \{0,1\}$ definován vztahem

$$|x\rangle \otimes |y\rangle \xmapsto{U_f} |x\rangle \otimes |y \oplus f(x)\rangle,$$

kde symbol $\oplus$ značí binární součet (součet v $\mathbb{Z}_2$). Všimněme si, že matice U_f permutuje čtyři bázové stavy $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, a je tedy zjevně unitární (speciálně platí $U_f \circ U_f = \mathrm{Id}$.

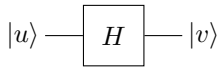
Uvedená konstrukce kvantového orákula je základem rozšířených schopností kvantového algoritmu. Je proto snadné nabýt dojmu, že kvantový algoritmus je úspěšnější díky uvolněnější definici orákula. Tento dojem je oprávněný jen z části. Kvantové orákulum nemá oproti klasickému žádnou výhodu, pokud jde o **bázové stavy** $|0\rangle$ a $|1\rangle$, na nichž je funkce definovaná. Rozšířené schopnosti nejsou dány ani tak konstrukcí orákula, jako typicky kvantovým faktem, že orákulum může zpracovávat i **superpozice**. Tím se také objevuje jistá „nedovolená“ informace o vnitřním fungování orákula, totiž že se vůči superpozicím stavů chová **lineárně**.

Po vzoru algoritmických schémat můžeme U_f zobrazit jako logické hradlo:



Tento zápis by neměl být směšován se schématem, které jsme použili pro polopropustné zrcadlo při popisu Machova-Zehnderova interferometru. Tam se jednalo o operátor jednokubitový, který by měl být jakožto hradlo nakreslen jako

kde $|v\rangle = H|u\rangle$, nebo ještě lépe jako

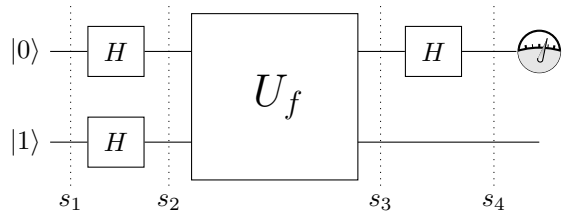


aby bylo jasné, že nám nezáleží na tom, jestli je operátor

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

realizován polopropustným zrcadlem, nebo jinak. Jak uvidíme, hraje právě tento operátor H v kvantových počítačích významnou roli a nazývá se *Hadamardův*.

Kvantový obvod realizující Deutschův algoritmus je poměrně jednoduchý. Sestává, kromě orákula U_f, ze tří Hadamardových hradel:



Na obrázku jsou svislými čarami vyznačeny čtyři fáze výpočtu. Na začátku je dvoukubitový registr ve stavu

$$s_1 = |01\rangle.$$

Ve druhé fázi dostáváme

$$s_2 = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Výsledek orákula samozřejmě záleží na funkci f. Nejjednodušším případem je $f(0) = f(1) = 0$, kdy U_f je identita (jednotková matice). Pak máme

$$s_3 = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Pokud $f(0) = f(1) = 1$, je akce U_f dána vztahem

$$|00\rangle \mapsto |01\rangle \qquad |01\rangle \mapsto |00\rangle \qquad |10\rangle \mapsto |11\rangle \qquad |11\rangle \mapsto |10\rangle.$$

Tedy

$$s_3 = \frac{1}{2}U_f(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \frac{1}{2}(|01\rangle - |00\rangle + |11\rangle - |10\rangle) =$$
$$= -\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Podobně můžeme postupovat v ostatních případech a dostaneme celkové vyjádření

$$s_3 = \begin{cases} \pm\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}, & \text{pokud } f(0) = f(1), \\ \\ \pm\frac{|0\rangle-|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}, & \text{pokud } f(0) \neq f(1). \end{cases}$$

Konečně

$$s_4 = \begin{cases} \pm|0\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}, & \text{pokud } f(0) = f(1), \\ \\ \pm|1\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}, & \text{pokud } f(0) \neq f(1). \end{cases}$$

Nyní je pravý čas **změřit první kubit**. Vlastní číslo příslušné $|0\rangle$ bude znamenat, že f je konstantní, vlastní číslo příslušné $|1\rangle$ opak.

Deutchův algoritmus ve své jednoduchosti ukazuje základní myšlenku všech kvantových algoritmů: superpozice stavů umožňuje v jistém smyslu spočítat mnoho hodnot současně. Všimněme si, že Hadamardova transformace způsobuje zpracování vyvážené superpozice obou hodnot. To na druhou stranu neznamená, že bychom

měli přímý přístup k jakékoli funkční hodnotě. Pokud bychom např. změřili první kubit ve fázi s_3, dostaneme bezcenný náhodný výsledek, nezávisle na funkci f.

Deutschův-Jozsův algoritmus

Obecnější forma uvedeného algoritmu se nazývá *Deutschův-Jozsův algoritmus*. Je dána funkce $f : \{0,1\}^n \to \{0,1\}$, která je buď konstantní, nebo balancovaná (tj. přesně polovina argumentů nabývá hodnoty 1 a druhá polovina hodnoty 0). Úkolem je opět zjistit, která z možností platí.

Obvod vypadá stejně jako v Deutschově algoritmu, pouze na vstupu je namísto $|0\rangle$ registr $|0\rangle^{\otimes n}$ a rovněž příslušné Hadamardovy transformace tohoto registru jsou tenzorově umocněny: $H^{\otimes n}$. Dostáváme tak poněkud komplikovanější popis jednotlivých fází. Na začátku máme stav

$$s_1 = |0^n 1\rangle.$$

a ve druhé fázi

$$s_2 = \left(\frac{1}{\sqrt{2}}\right)^n \bigotimes_{i=1}^{n}(|0\rangle + |1\rangle)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{1}{\sqrt{2}}\right)^n \left(\sum_{x\in\{0,1\}^n} |x\rangle\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

Analýzu případů z Deutschova algoritmu je možné zapsat úsporně. Všimněme si, že

$$U_f\left(|x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = |x\rangle\frac{|0\oplus f(x)\rangle - |1\oplus f(x)\rangle}{\sqrt{2}} = (-1)^{f(x)}|x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Po aplikaci orákula tedy dostáváme

$$s_3 = \left(\frac{1}{\sqrt{2}}\right)^n \left(\sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

Připomeňme, že platí

$$H^{\otimes n}|x\rangle = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{z\in\{0,1\}^n} (-1)^{x\cdot z}|z\rangle,$$

kde $x \cdot z = x_1x_2\ldots x_n \cdot z_1z_2\ldots z_n$ značí skalární součin vektorů cifer binárního rozvoje, tedy

$$\sum_{i=1}^{n} x_i z_i.$$

Pro závěrečnou fázi algoritmu tedy dostáváme

$$s_4 = \frac{1}{2^n}\left(\sum_{x\in\{0,1\}^n}\sum_{z\in\{0,1\}^n} (-1)^{x\cdot z+f(x)}|z\rangle\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

Jaké jsou možné výsledky měření prvního registru? Všimněme si, že každý bázový stav je v součtu 2^n-krát, s různými znaménky. Znaménka u stavu $|0^n\rangle$ ovšem závisejí pouze na $f(x)$. Je-li tedy f konstantní, je amplituda pravděpodobnosti stavu $|0^n\rangle$ rovna 1 nebo -1. Je-li naopak f balancovaná, kladných i záporných členů je stejný počet a amplituda pravděpodobnosti je 0. Výsledek měření tedy bude odpovídat stavu $|0^n\rangle$, právě když je f konstantní.

Všimněme si, že platí obecnější pravidlo, které zhruba říká, že pravděpodobnost naměření nuly je tím větší, čím je funkce f bližší konstantě.

Deutschův-Jozsův algoritmus umožňuje správnou odpověď po jediném dotazu na orákulum. To vůči deterministickému klasickému algoritmu znamená exponenciální zrychlení, protože ten potřebuje pro (jistou) odpověď $2^{n-1}+1$ dotazů. Existuje ovšem klasický probabilistický algoritmus s tolerovanou chybou $\frac{1}{2^k}$, kterému stačí k dotazů: po k náhodných dotazech odpovíme „konstantní“, právě když jsou všechny výsledky stejné. Možnost chyby existuje pouze u balancované funkce a je zjevně menší než požadovaná mez. Z tohoto hlediska, zejména když uvážíme náchylnost kvantových jevů k chybám, je zrychlení kvantového počítače pouze konstantní.