

Algoritmy založené na kvantové Fourierově transformaci

Libor Veis

1 Kvantová Fourierova transformace

2 Phase estimation

- Kvantová Fourierova transformace (QFT) je lineární transformace U na n qubitech, která převádí výpočetní bázeový stav $|j\rangle$ na superpozici podle

$$|j\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle \quad (1)$$

Úloha 1

Dokažte, že lineární transformace definovaná v rovnici (1) je unitární.

- Jak si ukážeme dále, QFT se dá realizovat s pomocí n^2 jedno- a dvou-qubitových hradel.
- Stav $|j\rangle$ vyjádříme v binární reprezentaci jako $|j_n j_{n-1} \dots j_1\rangle$, tedy

$$j = j_n 2^{n-1} + j_{n-1} 2^{n-2} + \dots + j_1 2^0 \quad (2)$$

- $j/2^n$ v exponentu rovnice (1) tedy odpovídá

$$\begin{aligned} \frac{j}{2^n} &= j_n 2^{-1} + j_{n-1} 2^{-2} + \dots + j_1 2^{-n} \\ &= 0.j_n j_{n-1} \dots j_1 \quad \text{binární frakce} \end{aligned} \quad (3)$$

- Postupnými úpravami lze rovnici (1) převést na vhodnější tvar pro reprezentaci kvantovým obvodem:

$$|j\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle \quad (4)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^1 \dots \sum_{k_n=0}^1 e^{2\pi i j (\sum_{l=1}^n k_l 2^{l-1-n})} |k_n \dots k_1\rangle \quad (5)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^1 \dots \sum_{k_n=0}^1 \bigotimes_{l=n}^1 e^{2\pi i j k_l 2^{l-1-n}} |k_l\rangle \quad (6)$$

$$= \frac{1}{\sqrt{2^n}} \bigotimes_{l=n}^1 \left[\sum_{k_l=0}^1 e^{2\pi i j k_l 2^{l-1-n}} |k_l\rangle \right] \quad (7)$$

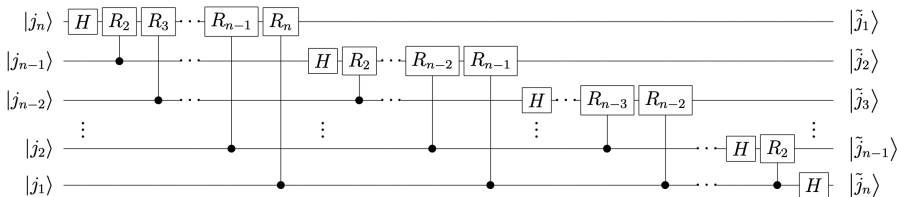
$$= \frac{1}{\sqrt{2^n}} \bigotimes_{l=n}^1 \left[|0\rangle + e^{2\pi i j 2^{l-1-n}} |1\rangle \right] \quad (8)$$

$$= \frac{\left(|0\rangle + e^{2\pi i 0 \cdot j_1} |1\rangle \right) \left(|0\rangle + e^{2\pi i 0 \cdot j_2 j_1} |1\rangle \right) \dots \left(|0\rangle + e^{2\pi i 0 \cdot j_n \dots j_1} |1\rangle \right)}{\sqrt{2^n}} \quad (9)$$

- Pokud zadefinujeme nové jedno-qubitové hradlo dávající příslušnou fázi stavu $|1\rangle$ následovně

$$R_j = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^j} \end{pmatrix} \quad (10)$$

Ize QFT implementovat kvantovým obvodem:



kde $|\tilde{j}_1\rangle$ značí $|0\rangle + e^{2\pi i 0 \cdot j_n \dots j_1} |1\rangle$, ... až k $|\tilde{j}_n\rangle = |0\rangle + e^{2\pi i 0 \cdot j_1} |1\rangle$. Všimněte si, že výsledné qubity jsou v opačném pořadí než v rovnici (9).

Úloha 2

Připomeňte si, kolik dalších CNOT hradel by bylo potřeba k řazení qubitů podle rovnice (9).

- Analýza QFT obvodu:
- Aplikace 1. Hadamardova hradla produkuje stav

$$\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle \right) |j_{n-1} \dots j_1\rangle, \quad (11)$$

Úloha 3

Ověřte, že $e^{2\pi i 0 \cdot j_n} = -1$ když $j_n = 1$ a $+1$ pokud $j_n = 0$, tedy že platí vztah (11).

- Následná controlled- R_2 rotace vytvoří

$$\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0 \cdot j_n j_{n-1}} |1\rangle \right) |j_{n-1} \dots j_1\rangle. \quad (12)$$

Analogicky, každá z kontrolovaných rotací $R_3 \dots R_n$ přidává další bit k fázi koeficientu prvního $|1\rangle$, což vede ke stavu

$$\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0 \cdot j_n j_{n-1} \dots j_1} |1\rangle \right) |j_{n-1} \dots j_1\rangle. \quad (13)$$

- Podobný postup na zbývajících qubitech dává konečný stav

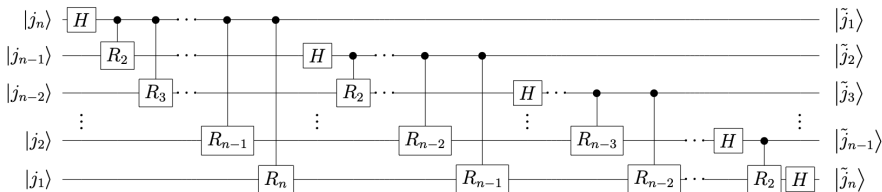
$$\frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2\pi i 0 \cdot j_n \dots j_1} |1\rangle \right) \left(|0\rangle + e^{2\pi i 0 \cdot j_{n-1} \dots j_1} |1\rangle \right) \dots \left(|0\rangle + e^{2\pi i 0 \cdot j_1} |1\rangle \right). \quad (14)$$

- Obvod kvantové Fourierovy transformace může být ve skutečnosti výrazně zjednodušen pomocí semiklasického (na měření založeného) přístupu.
- Protože Controlled- R_j hradla jsou diagonální matice, jejichž jediný nenulový prvek mimo jedničku na diagonále odpovídá bázeovému stavu $|11\rangle$, lze role obou qubitů prohodit.

$$\text{controlled-}R_j = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{2\pi i/2^j} \end{pmatrix} \Rightarrow \begin{array}{c} \bullet \\ | \quad | \\ \text{---} R_j \text{---} \\ \bullet \end{array} = \begin{array}{c} \text{---} R_j \text{---} \\ | \quad | \\ \bullet \end{array}$$

$\dots |11\rangle$

- Alternativní obvod:



- Protože se stav každého qubitu po aplikaci Hadamardova hradla nemění, může být měření, pokud následuje po QFT, provedeno ihned po tomto hradle.
- Místo kontrolovaných dvou-qubitových hradel lze provádět pouze *jedno-qubitová*, která závisí na výsledku předešlých měření - obrovská úspora!
- Hradla R_j odpovídají rotacím kolem osy z - všechny lze sloučit do jednoho:

$$R_z(\omega_k) = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i \omega_k} \end{pmatrix}, \quad (15)$$

jehož úhel ω_k závisí na výsledcích měření předešlých qubitů (q_i) podle

$$\omega_k = \sum_{i=2}^{n-k+1} \frac{q_{k+i-1}}{2^i}, \quad k : n \longrightarrow 1. \quad (16)$$

- Zjednodušený obvod QFT:

$$|q_k\rangle \rightarrow R_z(\omega_k) \rightarrow H \rightarrow \text{Measurement} = q_k$$

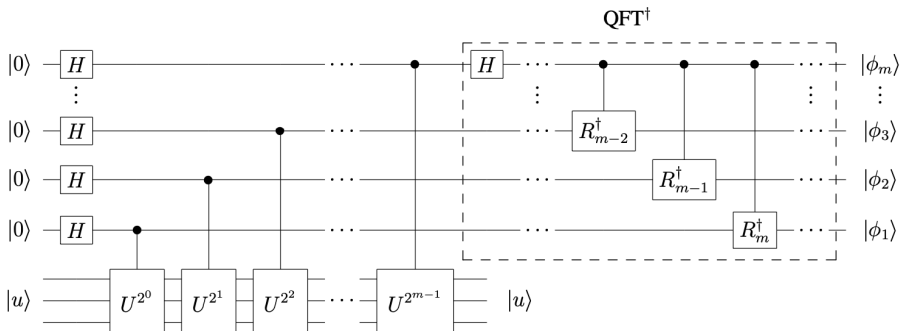
- Tato technika je obzvláště užitečná v souvislosti s algoritmem odhadu fáze (phase estimation, PEA), kde vede k formulaci jeho iterační verze (IPEA).

Phase estimation

- Phase estimation je kvantový algoritmus pro získání vlastního čísla unitárního operátoru $\hat{U}$ na základě daného počátečního odhadu odpovídajícího vlastního vektoru. Protože $\hat{U} = e^{i\hat{H}}$, kde $\hat{H}$ je hermitovský operátor $\Rightarrow$ kvantová obdoba klasické diagonalizace.
- Předpokládejme, že $|u\rangle$ je vlastní vektor $\hat{U}$ a že platí

$$\hat{U}|u\rangle = e^{2\pi i\phi}|u\rangle, \quad \phi \in (0, 1), \quad (17)$$

- ϕ je fáze odhadovaná algoritmem.
- Kvantový registr: $|\text{read-out-part}\rangle \otimes |u\rangle$



- Analýza PEA obvodu:
- Po aplikaci Hadamardových hradel na read-out části (m qubitů):

$$|\text{reg}\rangle = \frac{1}{\sqrt{2^m}} \left(|0\rangle + |1\rangle \right) \dots \left(|0\rangle + |1\rangle \right) |u\rangle = \frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} |j\rangle |u\rangle \quad (18)$$

- Po aplikaci sekvence kontrolovaných mocnin $\hat{U}$:

$$\begin{aligned} |\text{reg}\rangle &= \frac{1}{\sqrt{2^m}} \left(|0\rangle + e^{2\pi i 2^{m-1} \phi} |1\rangle \right) \left(|0\rangle + e^{2\pi i 2^{m-2} \phi} |1\rangle \right) \dots \left(|0\rangle + e^{2\pi i 2^0 \phi} |1\rangle \right) |u\rangle = \\ &= \frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} e^{2\pi i j \phi} |j\rangle |u\rangle = \frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} e^{2\pi i j \tilde{\phi} / 2^m} |j\rangle |u\rangle \end{aligned} \quad (19)$$

- Kde $\tilde{\phi} = 2^m \phi \dots$ celé číslo vyjádřené m bity

$$\frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} e^{2\pi i j \tilde{\phi} / 2^m} |j\rangle |u\rangle \xrightarrow{\text{inv. QFT}} |\tilde{\phi}\rangle \otimes |u\rangle \quad (20)$$

- Pokud se fáze ϕ nedá vyjádřit přesně pomocí m bitů

$$\phi = \phi' + \delta 2^{-m}, \quad \delta : 0 \leq \delta < 1 \quad (21)$$

- Dá se ukázat, že pravděpodobnost měření ϕ' (zaokrouhlení dolů) a $\phi' + 2^{-m}$ (zaokrouhlení nahoru) je

$$P_{\text{down}}(\delta = 1/2) + P_{\text{up}}(\delta = 1/2) = \frac{4}{\pi^2} + \frac{4}{\pi^2} > 0.81. \quad (22)$$

- Pokud $|u\rangle$ neznáme (což je typicky případ v kvantové chemii), můžeme algoritmus zahájit s libovolným počátečním odhadem $|\psi\rangle$, který lze rozložit do báze vlastních vektorů operátoru $\hat{U}$

$$|\psi\rangle = \sum_i c_i |u_i\rangle. \quad (23)$$

- Pravděpodobnost měření ϕ_i je úměrná $|c_i|^2$.
- PEA tvoří *základ Shorova algoritmu* pro faktorizaci celých čísel na součin prvočísel.

Úloha 4

Uvažujte matici

$$U = \begin{pmatrix} -1 & 0 \\ 0 & i \end{pmatrix},$$

pro kterou platí

#	eigenvalue	eigenvector	phase (ϕ)	binary representation of ϕ
1	$-1 = e^{i\pi}$	$ u_1\rangle = (1, 0)^T = 0\rangle$	0.5	$0.\phi_1\phi_2 = 0.10$
2	$i = e^{i\pi/2}$	$ u_2\rangle = (0, 1)^T = 1\rangle$	0.25	$0.\phi_1\phi_2 = 0.01$

Naimplementujte a vyzkoušejte v prostředí OpenQASM: <http://quantum.ibm.com/composer>
 algoritmus odhadu fáze podle následujícího obvodu

