Odhad fáze

Poučný pohled na použití Fourierovy transformace pro nalezení řádu prvku a, které jsme viděli v Shorově algoritmu, poskytuje postup tzv. *odhad fáze*. Jde o úkol spočítat vlastní číslo daného unitárního operátoru. Vlastní čísla unitárních operátorů přitom jsou tvaru $\exp[i\varphi]$, protože musejí mít velikost jedna; ptáme se tedy na číslo φ. Souvislost s hledáním řádu prvku je v tom, že pro matici U realizující násobení prvkem a řádu r platí $U^r = E$, a její vlastní čísla jsou proto tvaru

$$\lambda_p = \exp[2\pi i \frac{p}{r}], \quad p = 0, 1, \ldots, r-1.$$

Zjistit fázi nějakého vlastního čísla tedy přesně odpovídá nalezení zlomku, který hledáme v Shorově algoritmu. Je také snadné ověřit, že vlastní vektor $|u_p\rangle$ příslušný vlastnímu číslu λ_p je

$$|u_p\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} \exp[-2\pi i \frac{pj}{r}] |a^j\rangle.$$

Algoritmus pro odhad fáze ukážeme pro jednoduchý případ, že φ má konečný binární rozvoj $\varphi = 0.\varphi_1\varphi_2\ldots\varphi_m$. Nechť $|u\rangle$ je vlastní vektor příslušný vlastnímu číslu $\exp[2\pi i\varphi]$. Studujme umocňovací transformaci

$$W : |k\rangle|u\rangle \mapsto |k\rangle U^k|u\rangle,$$

kde $|k\rangle$ je bázový stav m-kubitového registru, a vyhodnoťme ji na rovnoměrné superpozici všech $|k\rangle$, tedy

$$\frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} |k\rangle|u\rangle \xmapsto{W} \frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} |k\rangle U^k|u\rangle = \frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} \exp[2\pi i k\varphi] |k\rangle|u\rangle.$$

Protože

$$\exp[2\pi i k\varphi] = \exp[2\pi i \frac{k \cdot \varphi_1\varphi_2\ldots\varphi_m}{2^m}],$$

vidíme, že stav prvního registru je nyní přesně $\mathrm{IFT}|\varphi_1\varphi_2\ldots\varphi_\mathrm{m}\rangle$, a aplikací DFT dostaneme $|\varphi_1\rangle|\varphi_2\rangle\cdots|\varphi_m\rangle$.

Tento případ odpovídá téměř přesně Shorovu algoritmu, všimněme si, že $\frac{1}{r}$ má konečný binární rozvoj délky m, právě když r dělí 2^m, což byl v Shorově algoritmu ideální případ. Zásadní rozdíl je v tom, že odhad fáze používá vlastní vektor $|u\rangle$, jehož konstrukce je bez znalosti φ, které teprve hledáme, nemožný.

Pokud aplikujeme algoritmus pro odhad fáze na nějaký stav $|v\rangle = \sum c_p|u_p\rangle$, kde $|u_p\rangle$ označuje vlastní vektor příslušný vlastnímu číslu $\exp[2\pi i\frac{p}{r}]$, dostaneme superpozici

$$\sum c_p |\lambda_{p,1}\rangle|\lambda_{p,2}\rangle\cdots|\lambda_{p,m}\rangle$$

a měřením získáme jedno z vlastních čísel s pravděpodobnostmi odpovídajícími amplitudám c_p.

Shorův algoritmus je aplikován na vektor $|1\rangle$. Souvislost mezi Shorovým algoritmem a odhadem fáze se uzavírá pozorováním, že

$$\frac{1}{\sqrt{r}} \sum_{p=0}^{r-1} |u_p\rangle = |1\rangle,$$

která vysvětluje, proč každý ze zlomků $p\frac{r}{M}$ získáme s pravděpodobností $\frac{1}{r}$.