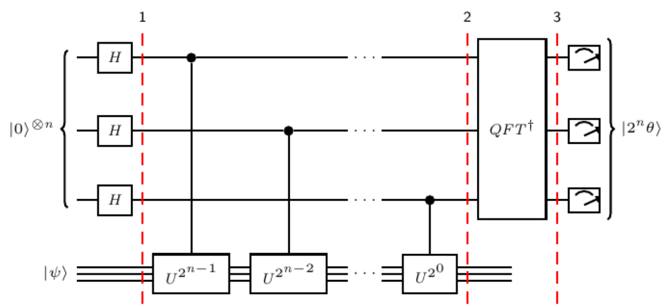
پردازش اطلاعات کوانتومی
نام و نام خانوادگی: مهدی وجهی
ارائه ۱۳
۸۱۰۱۰۱۵۵۸

۱ تخمین فاز

در این قسمت هدف این است که با اعمال عملگر روی مقدار ویژه آن θ را استخراج کنیم و تخمین بزنیم:

$$U\left|\psi\right\rangle = e^{2i\theta\pi}\left|\psi\right\rangle$$

مدار آن به شکل زیر است:



شکل ۱: مدار تخمین فاز

در هر مرحله بسته به شماره کیوبیت $U^{2^{n-i}}$ است که به دلیل حالت برهمنهی کنترل کننده پدیده $Phase\ Kickback$ رخ می دهد و مقدار آن به صورت زیر است:

$$U^{2^{n-i}}\left|\psi\right\rangle = U^{2^{n-i}-1}U\left|\psi\right\rangle = e^{2i\theta\pi}U^{2^{n-i}-1}\left|\psi\right\rangle = e^{2i\theta\pi 2^{n-i}}\left|\psi\right\rangle$$

بنابراین خروجی مدار به شکل زیر است:

$$\frac{1}{\sqrt{N}}(\left|0\right\rangle + e^{2i\theta\pi 2^{n-1}}\left|1\right\rangle) \otimes \cdots \otimes (\left|0\right\rangle + e^{2i\theta\pi 2^{0}}\left|1\right\rangle) \otimes \left|\psi\right\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{2^n-1} e^{2i\theta\pi k}\left|k\right\rangle \otimes \left|\psi\right\rangle$$

که با معکوس فوریه از آن j را به دست می آوریم که برابر است با:

$$\frac{1}{\sqrt{N}}\sum_{k=0}^{2^n-1} e^{2i\theta\pi k}\left|k\right\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{2^n-1} e^{2ijk\pi/2^n}\left|k\right\rangle \implies \theta = \frac{j}{2^n} \implies j = 2^n\theta$$

اگر $N\theta$ صحیح نباشد دیگر جواب قطعی نیست و مقدار نزدیک به آن را با احتمال ۴۰ درصد مشاهده می کنیم.

۲ یافتن دوره تناوب

برای یک تابع به شکل $f(x) = a^x \mod N$ دوره تناوب برابر با کمترین توانی است که $a^x = 1 \mod N$ بشود و این مقدار به علت اصل لانه کبوتری و قوانین حاکم بر میدان حداکثر $N-1$ است. این عدد را با r نمایش می دهیم.

حال در کیوبیت نیز همین است اگر ما $|1\rangle$ را ورودی دهیم با اعمال r بار عملگر تابع به ۱ می رسیم. اما این روش کارا نیست. ما می توانیم تمام ورودی ها را در حالت برهم نهی قرار دهیم و ورودی دهیم به صورت $|u_0\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|a^k \mod N\rangle$ است. چون مجدد با اعمال تابع همه تولید می شود مقدار ویژه ۱ است و کمکی نمی کند. اما اگر به آن یک فاز اضافه کنیم داریم:

$$\begin{aligned}
|u_1\rangle &= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2ik\pi/r}\left|a^k \mod N\right\rangle \\
U|u_1\rangle &= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2ik\pi/r}U\left|a^k \mod N\right\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2ik\pi/r}\left|a^{k+1} \mod N\right\rangle \\
&= \frac{e^{2i\pi/r}}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2i(k+1)\pi/r}\left|a^{k+1} \mod N\right\rangle = \frac{e^{2i\pi/r}}{\sqrt{r}}\sum_{k=1}^{r} e^{-2ik\pi/r}\left|a^k \mod N\right\rangle \\
&= \frac{e^{2i\pi/r}}{\sqrt{r}}(|1\rangle + \sum_{k=1}^{r-1} e^{-2ik\pi/r}\left|a^k \mod N\right\rangle) = \frac{e^{2i\pi/r}}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2ik\pi/r}\left|a^k \mod N\right\rangle = e^{2i\pi/r}|u_1\rangle
\end{aligned}$$

این موضوع برای باقی هم قابل تعمیم است و داریم:

$$|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2ik\pi s/r}\left|a^k \mod N\right\rangle \implies U|u_s\rangle = e^{2i\pi s/r}|u_s\rangle$$

حال همه این موارد را جمع می زنیم و داریم:

$$\begin{aligned}
\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle &= \frac{1}{r}\sum_{s=0}^{r-1}\sum_{k=0}^{r-1} e^{-2ik\pi s/r}\left|a^k \mod N\right\rangle = \frac{1}{r}\sum_{k=0}^{r-1}\sum_{s=0}^{r-1} e^{-2ik\pi s/r}\left|a^k \mod N\right\rangle \\
&= |1\rangle + \frac{1}{r}\sum_{k=1}^{r-1}(\sum_{s=0}^{r-1} e^{-2ik\pi s/r})\left|a^k \mod N\right\rangle = |1\rangle + \frac{1}{r}\sum_{k=1}^{r-1}(\frac{1-(e^{-2ik\pi s/r})^r}{1-e^{-2ik\pi s/r}})\left|a^k \mod N\right\rangle \\
&= |1\rangle + \frac{1}{r}\sum_{k=1}^{r-1}(\frac{1-1}{1-e^{-2ik\pi s/r}})\left|a^k \mod N\right\rangle = |1\rangle
\end{aligned}$$

در نهایت اگر ما $|1\rangle$ را ورودی بدهیم در واقع حالت بر هم نهی همه را ورودی داده ایم و جواب به صورت تصادفی یکی از مقادیر $0 \leq s < r$ $\frac{s}{r}$ است. با استفاده از مقادیر اندازه گیری شده و روش های کلاسیک می توانیم به صورت کارا r را حساب کنیم.

در نهایت ۶۰ درصد از مباحث را فهمیدم.