پردازش اطلاعات کوانتومی

نام و نام خانوادگی: مهدی وجهی

ارائه ۹ — ۸۱۰۱۰۱۵۵۸

۱ الگوریتم $Simon$

این الگوریتم موارد زیر را دارد $f(x) = f(x \oplus s), s \in \{0,1\}^n \wedge s \neq 0 \wedge f : \{0,1\}^n \rightarrow \{0,1\}^n$ هدف این الگوریتم پیدا کردن s است در روش کلاسیک ما باید بیش از نصف حالات را امتحان کنیم $(2^{n-1}+1)$ با الگوریتم های کلاسیک احتمالاتی این مقدار به $2^{n/2}$ کاهش پیدا می کند. حال گام های الگوریتم را می نویسیم:

$$|\psi_0\rangle = |0\rangle^{\otimes 2n} \implies |\psi_1\rangle = (H^{\otimes n} \otimes I)\,|0\rangle^{\otimes 2n} = \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^n}}\,|x\rangle\,|0\rangle^{\otimes n}$$

$$\implies |\psi_2\rangle = U_f \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^n}}\,|x\rangle\,|0\rangle^{\otimes n} = \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^n}}\,|xf(x)\rangle$$

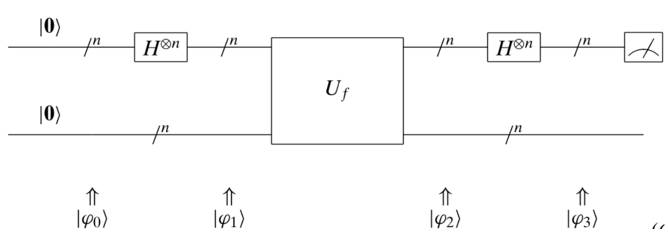
$$\implies |\psi_3\rangle = (H^{\otimes n} \otimes I) \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^n}}\,|xf(x)\rangle = \sum_{x\in\{0,1\}^n} \sum_{z\in\{0,1\}^n} \frac{1}{2^n}(-1)^{x.z}\,|zf(x)\rangle$$

$$= \sum_{z\in\{0,1\}^n} |z\rangle\,\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x.z}\,|f(x)\rangle \qquad X' := \{x \in \{0,1\}^n \mid x < (x \oplus s)\}$$

$$= \sum_{z\in\{0,1\}^n} |z\rangle\,\frac{1}{2^n} \sum_{x\in X'} \Big((-1)^{x.z}\,|f(x)\rangle + (-1)^{(x\oplus s).z}\,|f(x\oplus s)\rangle\Big) \qquad f(x) = f(x\oplus s)$$

$$= \sum_{z\in\{0,1\}^n} |z\rangle\,\frac{1}{2^n} \sum_{x\in X'} \Big((-1)^{x.z}(1+(-1)^{s.z})\,|f(x)\rangle\Big)$$

$$= \begin{cases} 0 & s.z = 1 \quad mod\ 2 \\ \sum_{z\in\{0,1\}^n} |z\rangle\,\frac{1}{2^{n-1}} \sum_{x\in X'} (-1)^{x.z}\,|f(x)\rangle & s.z = 0 \quad mod\ 2 \end{cases}$$



شکل ۱: مدار الگوریتم سیمون

بنابراین تنها حالت ممکن $s.z = 0 \quad mod\ 2$ است. هدف به دست آوردن s بود. برای به دست آوردن تمام ارقام s ما نیاز به n معادله مستقل برای به دست آوردن تمام n رقم آن داریم. معادله های خود را همان $s.z = 0 \quad mod\ 2$ در نظر می گیریم و از $|z\rangle$ که n بیت بالایی مدار است نمونه میگیریم و معادله را تشکیل می دهیم. این کار را به مقدار لازم انجام میدهیم تا به $n-1$ معادله مستقل خود برسیم . و سپس دستگاه معادلات را با آنها حل می کنیم. از نظر آماری می توان تقریبا با $n-1$ اجرا به معادلات رسید.

$$\begin{gathered}
z_1^1.s_1 + \cdots + z_n^1.s_n = 0 \quad mod\ 2 \\
z_1^2.s_1 + \cdots + z_n^2.s_n = 0 \quad mod\ 2 \\
\vdots \\
z_1^{n-1}.s_1 + \cdots + z_n^{n-1}.s_n = 0 \quad mod\ 2
\end{gathered}$$

توجه کنید حالت های $z = 0$ ، $s = 0$ بدیهی هستند و مطلوب ما نیستند پس مثلا اگر حالت $z = 0$ را اندازه بگیریم دور میریزیم.

در نهایت چیزی در حدود ۸۰ درصد مباحث را فهم کردم.