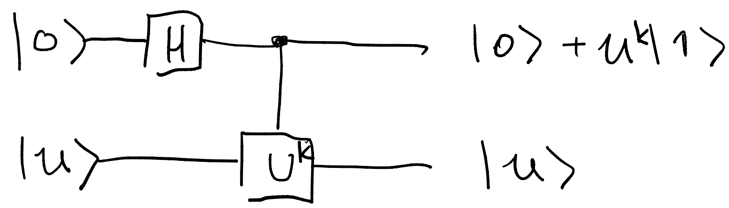
keskiviikko 10. toukokuuta 2023 9.48



$$u = e^{i2\pi\varphi}, \quad \varphi \in \mathbb{R}$$

$$u^2 = \left(e^{i2\pi\varphi}\right)^2 = e^{i2\pi \cdot 2\varphi}$$

$$|0\rangle \otimes |u\rangle \xmapsto{H\otimes I} \left(|0\rangle + |1\rangle\right) \otimes |u\rangle = |0\rangle|u\rangle + |1\rangle|u\rangle$$

$$\xmapsto{cU} |0\rangle|u\rangle + |1\rangle \underbrace{U^k|u\rangle}_{u} = |0\rangle|u\rangle + u^k|1\rangle|u\rangle$$

$$= \left(|0\rangle + u^k|1\rangle\right)|u\rangle$$

$$\varphi = \varphi_1 \cdot \frac{1}{2} + \varphi_2 \cdot \frac{1}{2^2} + \varphi_3 \cdot \frac{1}{2^3} + \dots$$

$$2\varphi = \underline{\underline{\varphi_1}} + \varphi_2 \cdot \frac{1}{2} + \varphi_3 \cdot \frac{1}{2^2} + \dots$$

$$2^\ell \varphi = \underbrace{\text{integer part}}_{\text{doesn't contribute to } e^{i2\pi \cdot 2^\ell \varphi}} + \varphi_{\ell+1} \cdot \frac{1}{2} + \varphi_{\ell+2} \cdot \frac{1}{4} + \dots$$

$$U|y\rangle = |yx \bmod N\rangle$$

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-i2\pi \frac{ks}{r}} |x^k \bmod N\rangle$$

$$U|\underline{\underline{u_s}}\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-i2\pi \frac{ks}{r}} |x^{k+1} \bmod N\rangle, \quad s = 0, \dots, r-1$$

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \underbrace{e^{-i2\pi \frac{(k-1)s}{r}}} |x^k \bmod N\rangle$$

$$= e^{i2\pi \frac{s}{r}} e^{-i2\pi \frac{ks}{r}}$$

$$= \underbrace{e^{i2\pi \frac{s}{r}}} \; e^{-i2\pi \frac{\ }{r}}$$

$$= e^{i2\pi\frac{s}{r}} |u_s\rangle \longrightarrow \frac{s}{r} \longrightarrow r$$

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = \frac{1}{r} \sum_{k=0}^{r-1} \underbrace{\left[\sum_{s=0}^{r-1} e^{-i2\pi \frac{ks}{r}} \right]}_{= \begin{cases} r & \text{if } k=0 \\ 0 & \text{otherwise} \end{cases}} |x^k \bmod N\rangle$$

$$= |1\rangle$$

$$H^{\otimes n} \left(2|0\rangle\langle 0| - I \right) H^{\otimes n}$$

$$= 2 \underbrace{H^{\otimes n}|0\rangle}_{|\psi\rangle} \underbrace{\langle 0| H^{\otimes n}}_{\langle\psi|} - \underbrace{(H^2)^{\otimes n}}_{I} = 2|\psi\rangle\langle\psi| - I$$

$$H^{\otimes n}|0\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle = |\psi\rangle$$

$$(2|\psi\rangle\langle\psi| - I)|\psi\rangle = 2|\psi\rangle\underbrace{\langle\psi|\psi\rangle}_{=1} - |\psi\rangle = |\psi\rangle$$

$$|\psi_\perp\rangle \text{ s.t. } \langle\psi_\perp|\psi\rangle = 0$$

$$(2|\psi\rangle\langle\psi| - I)|\psi_\perp\rangle = 2|\psi\rangle\underbrace{\langle\psi|\psi_\perp\rangle}_{=0} - |\psi_\perp\rangle = -|\psi_\perp\rangle$$