Shor’s Algorithm

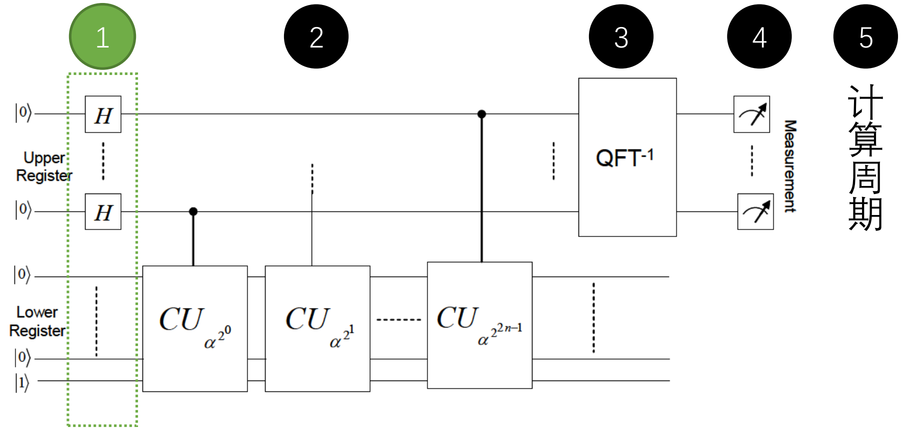
第6讲：Shor算法原理三

4. 态的演化

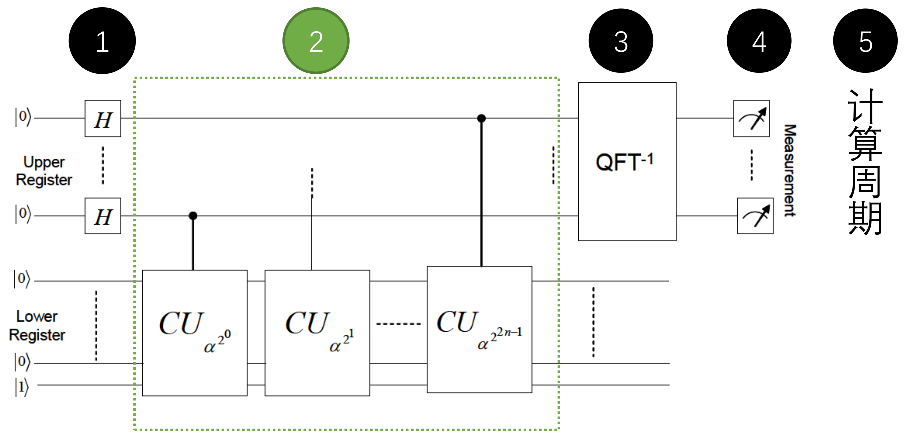
本源量子

给定$Q=2^t, t=2n$，$f(x)=a^x mod\ N$ 周期为r

1 初态： $|\varphi\rangle=\frac{1}{\sqrt{Q}}\sum_{i=0}^{Q-1}|\ i\ \rangle|1\rangle$



给定$Q=2^t, t=2n$， $f(x)=a^x mod\ N$ 周期为r



1 初态： $|\varphi\rangle=\frac{1}{\sqrt{Q}}\sum_{i=0}^{Q-1}|\,i\,\rangle|1\rangle$

2 经过模指线路后：

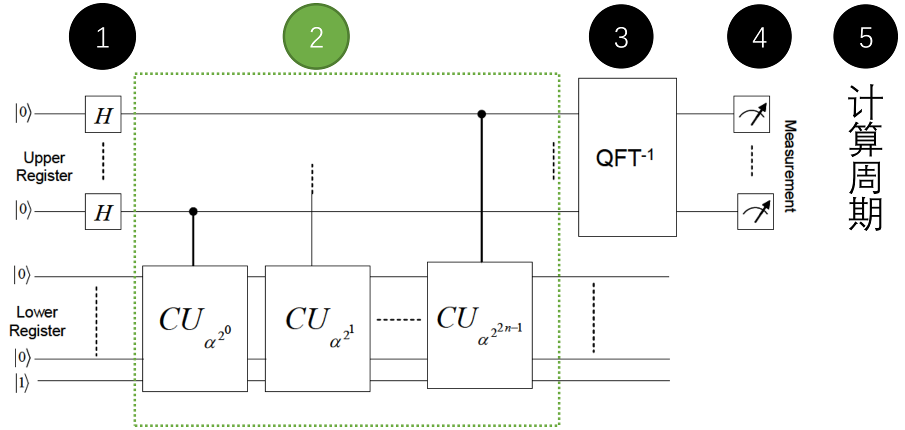
$$
\begin{aligned}
|\varphi\rangle = \frac{1}{\sqrt{Q}}(& \,|0\rangle|f(0)\rangle+|r\rangle|f(0)\rangle+\cdots+|mr\rangle|f(0)\rangle \\
& +|1\rangle|f(1)\rangle+|1+r\rangle|f(1)\rangle+\cdots+|1+mr\rangle|f(1)\rangle \\
& +|2\rangle|f(2)\rangle+|2+r\rangle|f(2)\rangle+\cdots+|2+mr\rangle|f(2)\rangle \\
& \cdots \\
& +|r-1\rangle|f(r-1)\rangle+|r-1+r\rangle|f(r-1)\rangle+\cdots+\ |r-1+mr\rangle|f(r-1)\rangle\ )
\end{aligned}
$$

$$
=\frac{1}{\sqrt{Q}}\sum_{i=0}^{r-1}\sum_{j=0}^{m}|\,i+jr\,\rangle|f(i)\rangle
$$

给定$Q=2^t, t=2n$， $f(x)=a^x mod\ N$ 周期为r

1 初态： $|\varphi\rangle=\frac{1}{\sqrt{Q}}\sum_{i=0}^{Q-1}|\ i\ \rangle|1\rangle$

2 经过模指线路后：



$$|\varphi\rangle=\frac{1}{\sqrt{Q}}(\ |0\rangle|f(0)\rangle+|r\rangle|f(0)\rangle+\cdots+|mr\rangle|f(0)\rangle$$

$$+|1\rangle|f(1)\rangle+|1+r\rangle|f(1)\rangle+\cdots+|1+mr\rangle|f(1)\rangle$$

$$+|2\rangle|f(2)\rangle+|2+r\rangle|f(2)\rangle+\cdots+|2+mr\rangle|f(2)\rangle$$

$r\times m\approx Q$

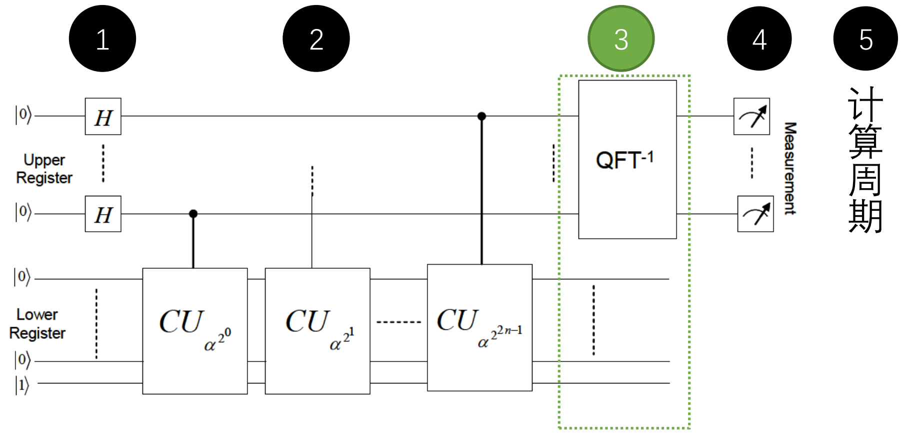
这里，已经体现周期的存在

$$\cdots$$

$$+|r-1\rangle|f(r-1)\rangle+|r-1+r\rangle|f(r-1)\rangle+\cdots+\ |r-1+mr\rangle|f(r-1)\rangle\ )$$

$$=\frac{1}{\sqrt{Q}}\sum_{i=0}^{r-1}\sum_{j=0}^{m}|\ i+jr\ \rangle|f(i)\rangle$$

给定$Q=2^t, t=2n$， $f(x)=a^x mod\ N$ 周期为r



1 初态： $|\varphi\rangle=\frac{1}{\sqrt{Q}}\sum_{i=0}^{Q-1}|\,i\,\rangle|1\rangle$

2 经过模指线路后：

$$
\begin{aligned}
|\varphi\rangle=\frac{1}{\sqrt{Q}}(\ &|0\rangle|f(0)\rangle+|r\rangle|f(0)\rangle+\cdots+|mr\rangle|f(0)\rangle\\
&+|1\rangle|f(1)\rangle+|1+r\rangle|f(1)\rangle+\cdots+|1+mr\rangle|f(1)\rangle\\
&+|2\rangle|f(2)\rangle+|2+r\rangle|f(2)\rangle+\cdots+|2+mr\rangle|f(2)\rangle\\
&\cdots\\
&+|r-1\rangle|f(r-1)\rangle+|r-1+r\rangle|f(r-1)\rangle+\cdots+|r-1+mr\rangle|f(r-1)\rangle\ )
\end{aligned}
$$

$r\times m\approx Q$

$$=\frac{1}{\sqrt{Q}}\sum_{i=0}^{r-1}\sum_{j=0}^{m}|\,i+jr\,\rangle|f(i)\rangle$$

3 上半部分做QFT^{-1}后

$$|\,i+jr\,\rangle\rightarrow\frac{1}{\sqrt{Q}}\sum_{k=0}^{Q-1}w^{k(i+jr)}|k\rangle\,,w=e^{\frac{-2\pi i}{Q}}$$

$$|\varphi\rangle=\frac{1}{Q}\sum_{i=0}^{r-1}\sum_{j=0}^{m}\sum_{k=0}^{Q-1}w^{k(i+jr)}|k\rangle|f(i)\rangle,$$ 共$r\times Q$个态

给定$Q = 2^t, t = 2n$， $f(x) = a^x \bmod N$ 周期为r

3 上半部分做QFT^{-1}后

$$| i + jr \rangle \rightarrow \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} w^{k(i+jr)} |k\rangle , w = e^{\frac{-2\pi i}{Q}}$$

$$|\varphi\rangle = \frac{1}{Q} \sum_{i=0}^{r-1} \sum_{j=0}^{m} \sum_{k=0}^{Q-1} w^{k(i+jr)} |k\rangle |f(i)\rangle,$$ 共$r \times Q$个态

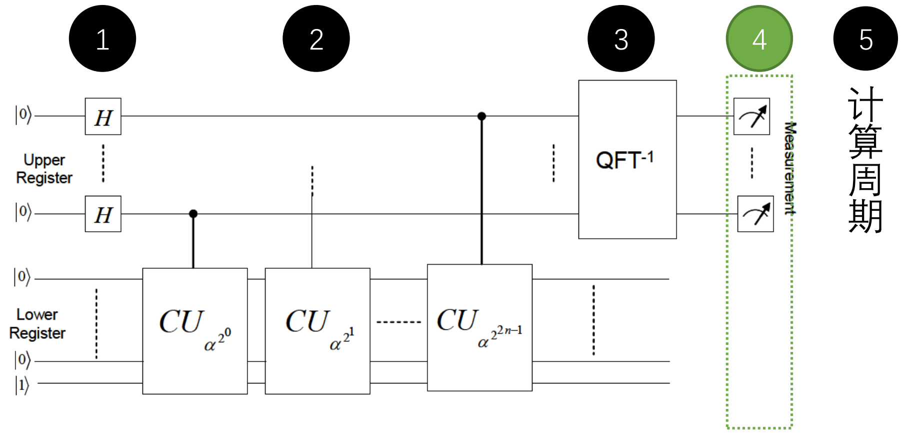
4 此时$|k\rangle|f(i)\rangle$的复振幅$F_k = \frac{1}{Q} \sum_{j=0}^{m} w^{k(i+jr)} = \frac{1}{Q} w^{ki} \frac{1-w^{mkr}}{1-w^{kr}}$

此时测量$|k\rangle$态的概率为 $P_k = \sum_{i=0}^{r-1} |F_k|^2 = \frac{r}{Q^2} \times \left| \frac{1-w^{mkr}}{1-w^{kr}} \right|^2$

$$w = e^{\frac{-2\pi i}{Q}}, \left| \frac{1-w^{mkr}}{1-w^{kr}} \right|^2 = \frac{1-\cos(m\theta)}{1-\cos(\theta)}, \theta = \frac{k \times r}{Q} \times 2\pi$$

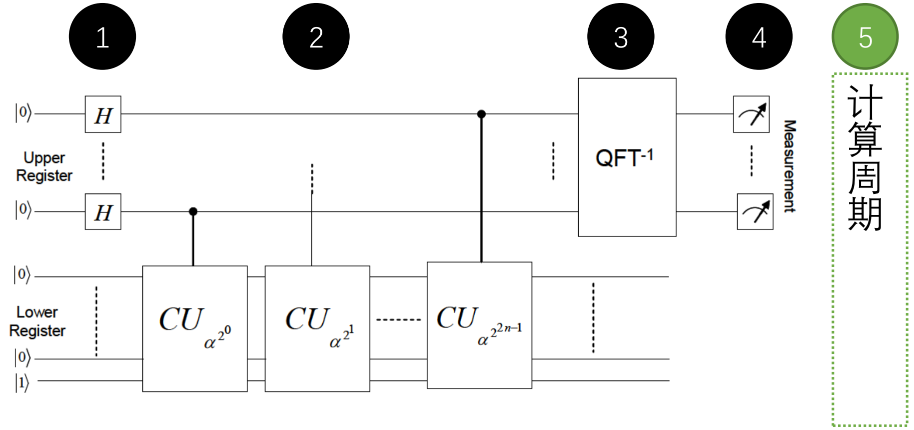
$P_k = \frac{r}{Q^2} \times \frac{1-\cos(m\theta)}{1-\cos(\theta)}$, $\theta = 2\pi \times s$,s为整数时， P_k取最大值

$$P_{k\max} = \frac{r}{Q^2} \times m^2 \approx \frac{1}{r}, m \times r \approx Q$$



此时，已经找到了与r的关系

给定$Q=2^t, t=2n$，$f(x)=a^x \bmod N$ 周期为r



3 上半部分做QFT^{-1}后

$$|i+jr\rangle \rightarrow \frac{1}{\sqrt{Q}}\sum_{k=0}^{Q-1} w^{k(i+jr)}|k\rangle, w=e^{\frac{-2\pi i}{Q}}$$

$$|\varphi\rangle=\frac{1}{Q}\sum_{i=0}^{r-1}\sum_{j=0}^{m}\sum_{k=0}^{Q-1} w^{k(i+jr)}|k\rangle|f(i)\rangle,$$ 共$r\times Q$个态

4 此时$|k\rangle|f(i)\rangle$的复振幅$F_k=\frac{1}{Q}\sum_{j=0}^{m} w^{k(i+jr)}=\frac{1}{Q}w^{ki}\frac{1-w^{mkr}}{1-w^{kr}}$

此时测量$|k\rangle$态的概率为 $P_k=\sum_{i=0}^{r-1}|F_k|^2=\frac{r}{Q^2}\times\left|\frac{1-w^{mkr}}{1-w^{kr}}\right|^2$

$$w=e^{\frac{-2\pi i}{Q}},\ \left|\frac{1-w^{mkr}}{1-w^{kr}}\right|^2=\frac{1-\cos(m\theta)}{1-\cos(\theta)},\ \theta=\frac{k\times r}{Q}\times 2\pi$$

$P_k=\frac{r}{Q^2}\times\frac{1-\cos(m\theta)}{1-\cos(\theta)}$, $\theta=2\pi\times s$,s为整数时，P_k取最大值

$$P_{k\max}=\frac{r}{Q^2}\times m^2\approx\frac{1}{r},m\times r\approx Q$$

此时，已经找到了与r的关系

5 最后测量的$|k\rangle$,测量结果满足 $\theta=\frac{k\times r}{Q}$为整数或接近整数，根据

$\frac{k}{Q}\sim\sim\frac{s}{r}$ 对$\frac{k}{Q}$做连分数分解，得到r的值，即得到$f(x)=a^x \bmod N$的周期

给定$Q = 2^t, t = 2n$，$f(x) = a^x mod\ N$ 周期为r

3 上半部分做QFT^{-1}后

$$| i + jr \rangle \to \frac{1}{\sqrt{Q}}\sum_{k=0}^{Q-1} w^{k(i+jr)}|k\rangle, w = e^{\frac{-2\pi i}{Q}}$$

$$|\varphi\rangle = \frac{1}{Q}\sum_{i=0}^{r-1}\sum_{j=0}^{m}\sum_{k=0}^{Q-1} w^{k(i+jr)}|k\rangle|f(i)\rangle,$$ 共$r \times Q$个态

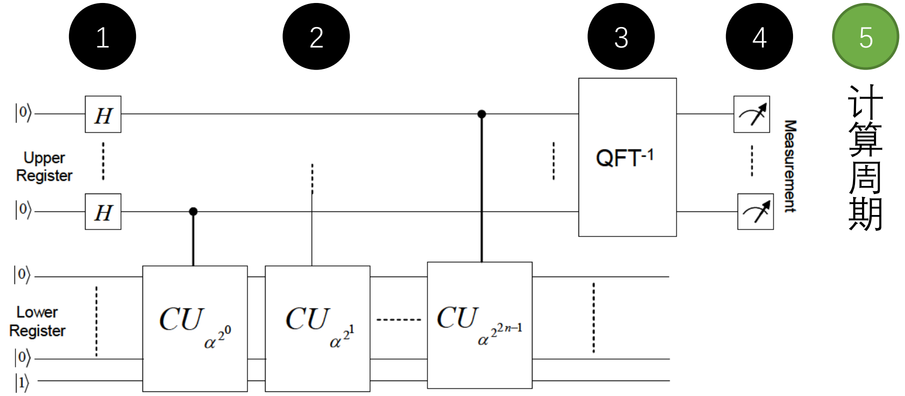
4 此时$|k\rangle|f(i)\rangle$的复振幅$F_k = \frac{1}{Q}\sum_{j=0}^{m} w^{k(i+jr)} = \frac{1}{Q} w^{ki}\frac{1-w^{mkr}}{1-w^{kr}}$

此时测量$|k\rangle$态的概率为 $P_k = \sum_{i=0}^{r-1}|F_k|^2 = \frac{r}{Q^2} \times \left|\frac{1-w^{mkr}}{1-w^{kr}}\right|^2$

$$w = e^{\frac{-2\pi i}{Q}}, \left|\frac{1-w^{mkr}}{1-w^{kr}}\right|^2 = \boxed{\frac{1-\cos(m\theta)}{1-\cos(\theta)}}, \theta = \frac{k \times r}{Q} \times 2\pi$$

$P_k = \frac{r}{Q^2} \times \frac{1-\cos(m\theta)}{1-\cos(\theta)}$, $\theta = 2\pi \times s$,s为整数时，P_k取最大值

$$P_{kmax} = \frac{r}{Q^2} \times m^2 \approx \frac{1}{r}, m \times r \approx Q$$



计算周期

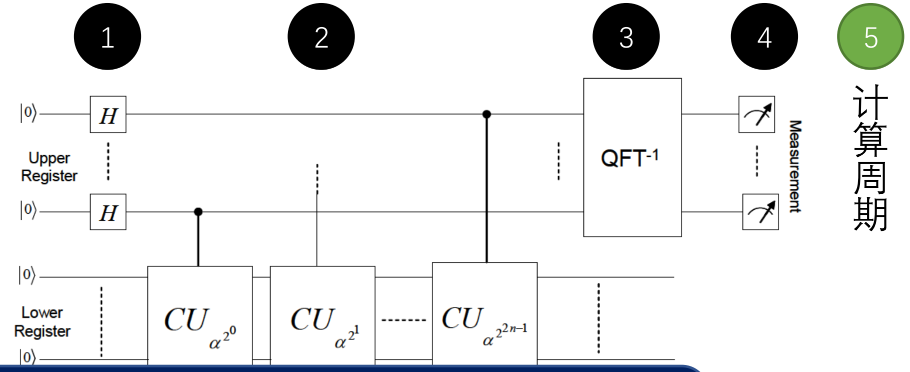
此时，已经找到了与r的关系

5 最后测量的$|k\rangle$,测量结果满足 $\theta = \frac{k \times r}{Q}$为整数或接近整数，根据$\frac{k}{Q} \sim\sim \frac{s}{r}$ 对$\frac{k}{Q}$做连分数分解，得到r的值，即得到$f(x) = a^x mod\ N$的周期

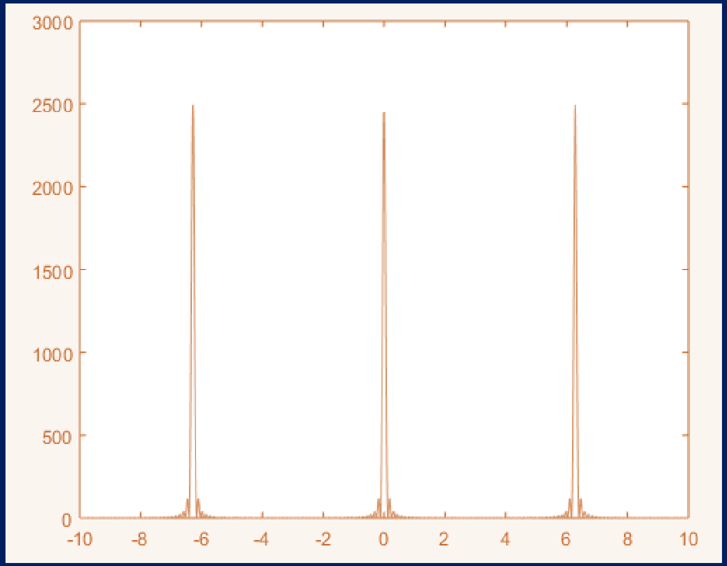
给定$Q=2^t, t=2n$，$f(x)=a^x mod\ N$ 周期为r

3 上半部分做QFT^{-1}后

$$|\,i+jr\,\rangle \rightarrow \frac{1}{\sqrt{Q}}\sum_{k=0}^{Q-1} w^{k(i+jr)}|k\rangle, w=e^{\frac{-2\pi i}{Q}}$$



4



$$\frac{1-\cos(m\times\theta)}{1-\cos(\theta)}$$

注：m=50

5 最后测量的$|k\rangle$,测量结果满足 $\theta=\frac{k\times r}{Q}$为整数或接近整数，根据

$\frac{k}{Q}\sim\sim\frac{s}{r}$ 对$\frac{k}{Q}$做连分数分解，得到r的值，即得到$f(x)=a^x mod\ N$的周期

4. 确认周期

本 源 量 子

$\frac{k}{Q}$是$\frac{c}{r}$的近似，将$\frac{k}{Q}$通过连分数方法发现 r；

连分数分解

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

$$a_0 + \frac{1}{a_1} \rightarrow a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}} \rightarrow \cdots\cdots \rightarrow \frac{c}{r}$$

$N = 77$

$N = 11 \times 7$, 取$f(x) = 3^x \, mod \, 77, r = 30$

Shor算法中上部分取14(即$2 \times 7 = 14$)个量子比特。

$Q = 2^{14}$,最后经过逆QFT后有

$$p_k = \frac{1}{Q \times m} \times \frac{1 - \cos(m\theta)}{1 - \cos(\theta)}, \theta = \exp\left(\frac{2\pi \times \mathrm{kr}}{Q}\right), m \times r \sim Q, p_{kmax} = \frac{1}{m}$$

$$\frac{k}{Q} \to \frac{0}{r}, \frac{1}{r}, \frac{2}{r} \dots \frac{r-1}{r},$$

$N = 77$

预计测量到的k值

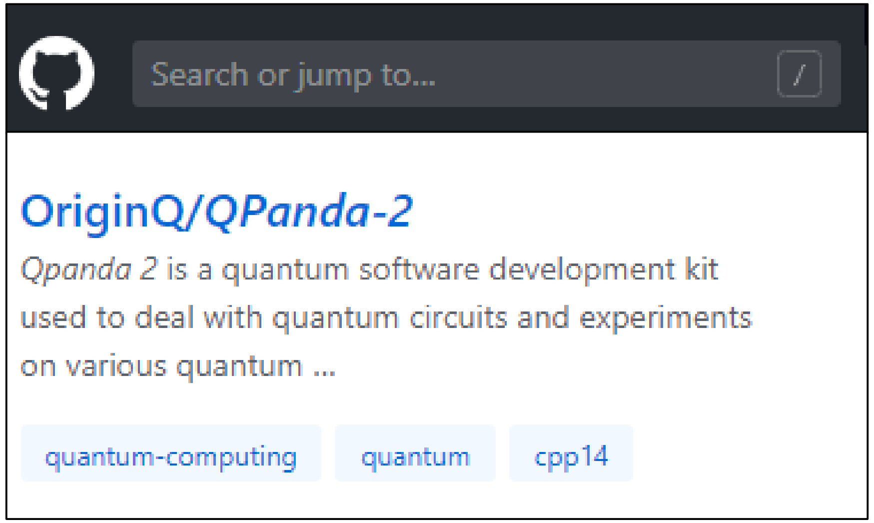
s/r	k=Qs/r	连分数逼近				结果
1/30	546	1/30				30
2/30	1092	1/15				15
7/30	3823	1/4	1/5	4/17	7/30	30
11/30	6007	1/2	3/8	11/30		30
11/30	6008	1/2	3/8	7/19	11/30	30
17/30	9284	1	1/2	4/7	17/30	30

$Q \quad r, r, r \cdots r,$

本源量子

追本溯源 高掌远跖

https://www.originqc.com.cn



研究致谢：陈昭昀，薛程，李叶