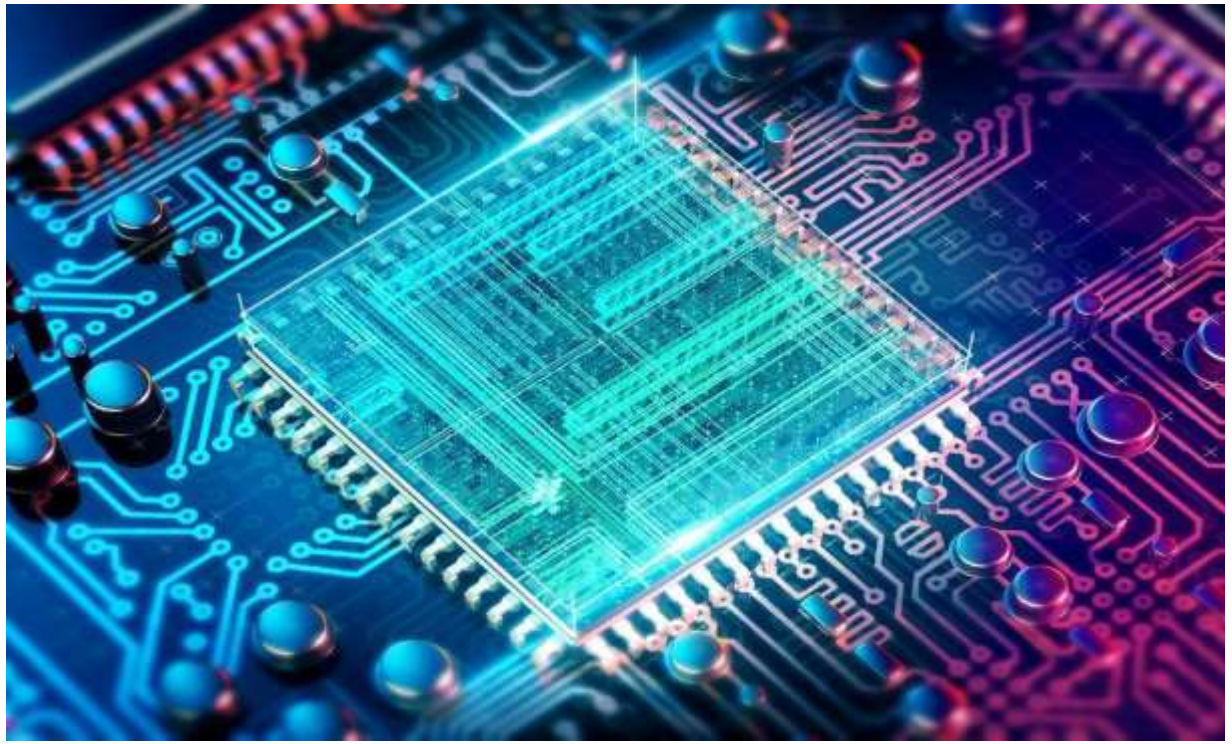
Quantum Information and Quantum Computation

Yuanyuan Chen

College of Physical Science and Technology
Xiamen University
Email: chenyy@xmu.edu.cn
http://qolab.xmu.edu.cn

Lecture 11

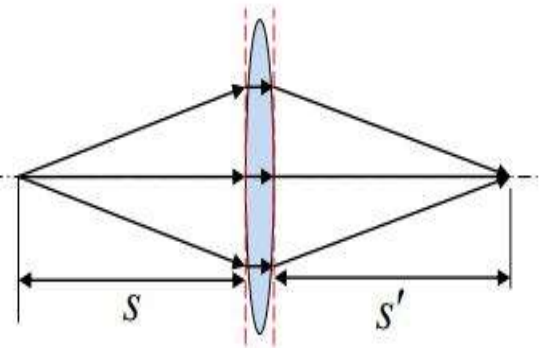
Quantum Fourier transform



A great discovery of quantum computation has been that some such transformstions can be computed much faster on a quantum computer than on a classical computer, a discovery which has enabled the construction of fast algorithms for quantum computers.

Discrete Fourier transform

$$F[n] = \sum_{k=0}^{N-1} f[k] e^{-j\frac{2\pi}{N}nk} \qquad (n = 0 : N-1)$$



入射场：球面波 $\tilde{U}_1 = A_1 \mathrm{e}^{ik\frac{x^2+y^2}{2s}}$

出射场：

$$\tilde{U}_2 = A_1 \mathrm{e}^{ik\frac{x^2+y^2}{2s}} \mathrm{e}^{-ik\frac{x^2+y^2}{2F}}$$

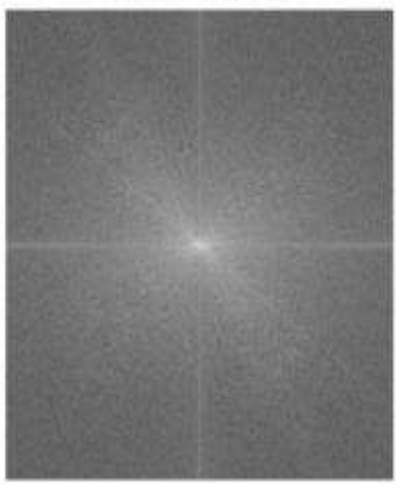
$$= A_1 \mathrm{e}^{-ik\left(\frac{x^2+y^2}{2F}-\frac{x^2+y^2}{2s}\right)}$$

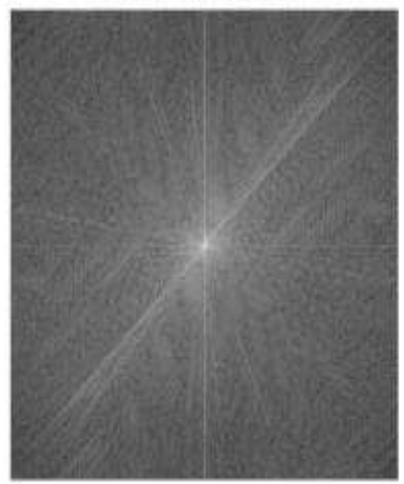
$$= A_1 \mathrm{e}^{-ik\frac{x^2+y^2}{2}\left(\frac{1}{F}-\frac{1}{s}\right)}$$

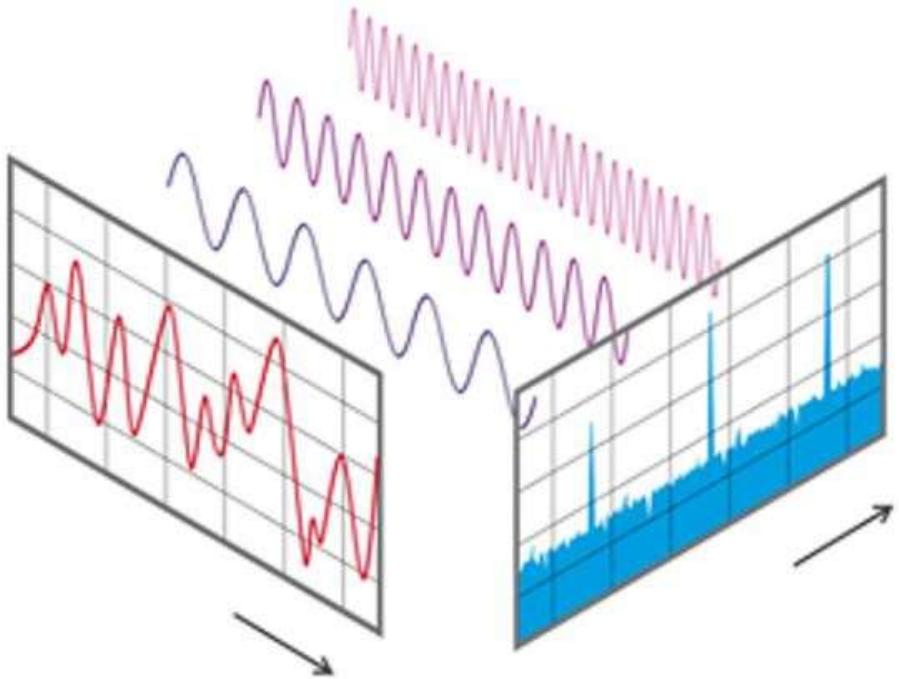
出射场特征：汇聚到轴上s'处的球面波。

球心位置 $s' = \left(\frac{1}{F}-\frac{1}{s}\right)^{-1} = \frac{sF}{s-F}$ ⟹ $\frac{F}{s}+\frac{F}{s'}=1$

Gauss 公式

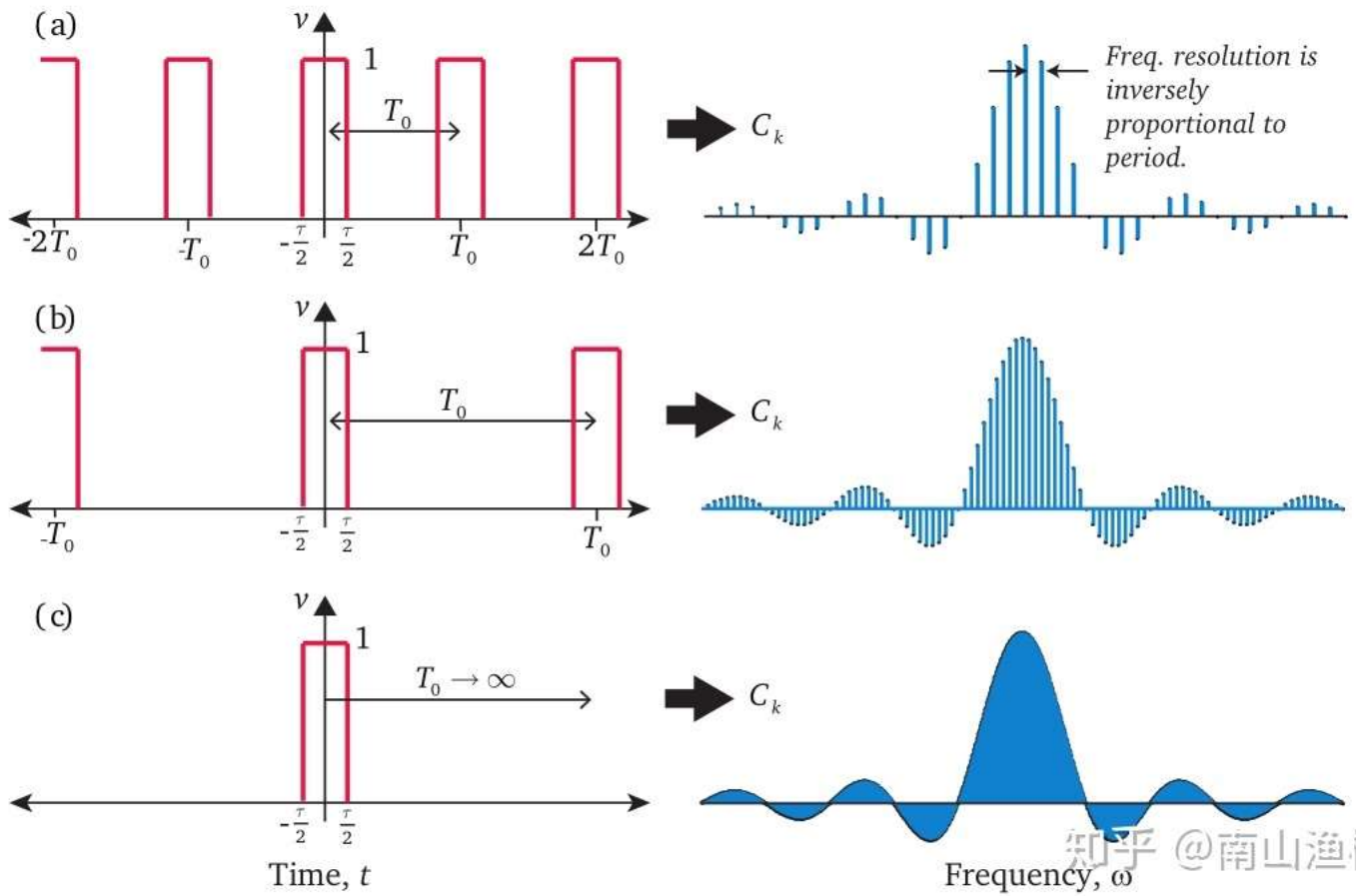


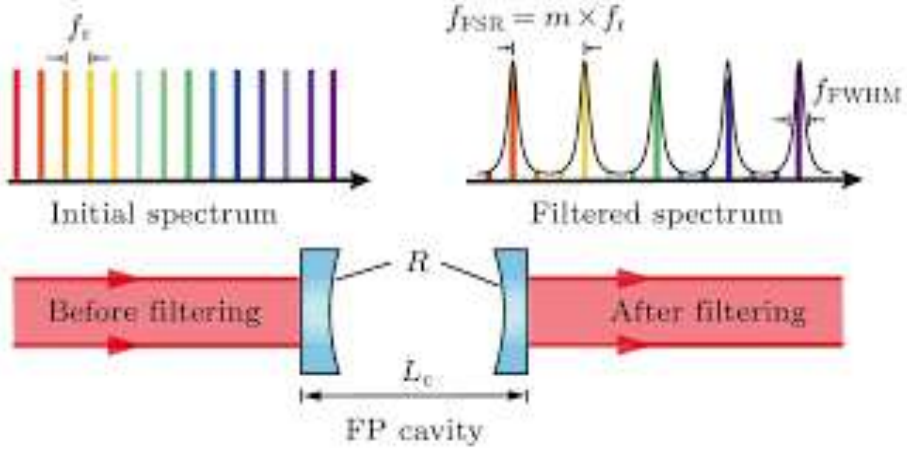




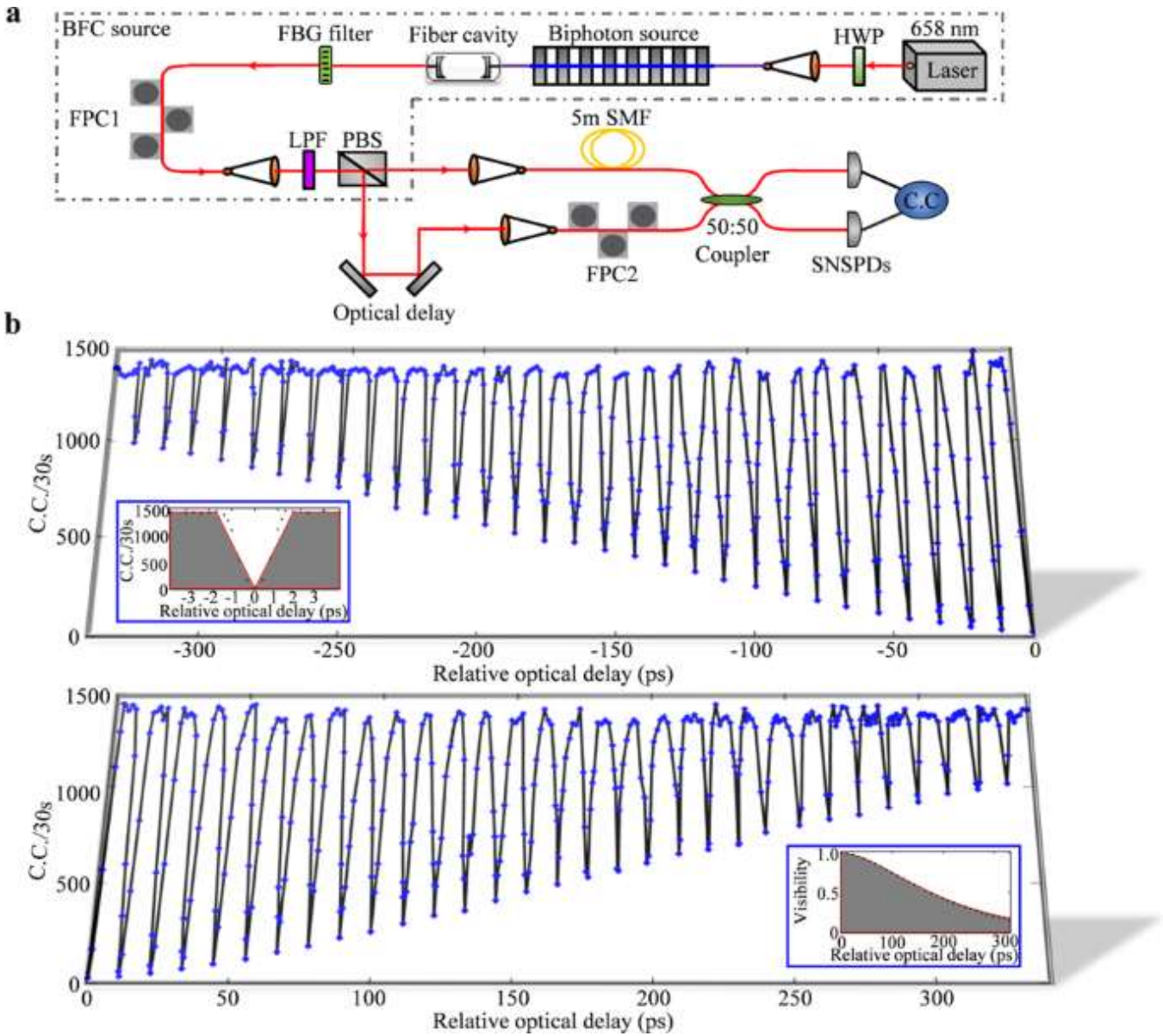
time, x
f(x)
一维信号

frequency, u
F(u)Re
一维幅谱





Spectral filtering

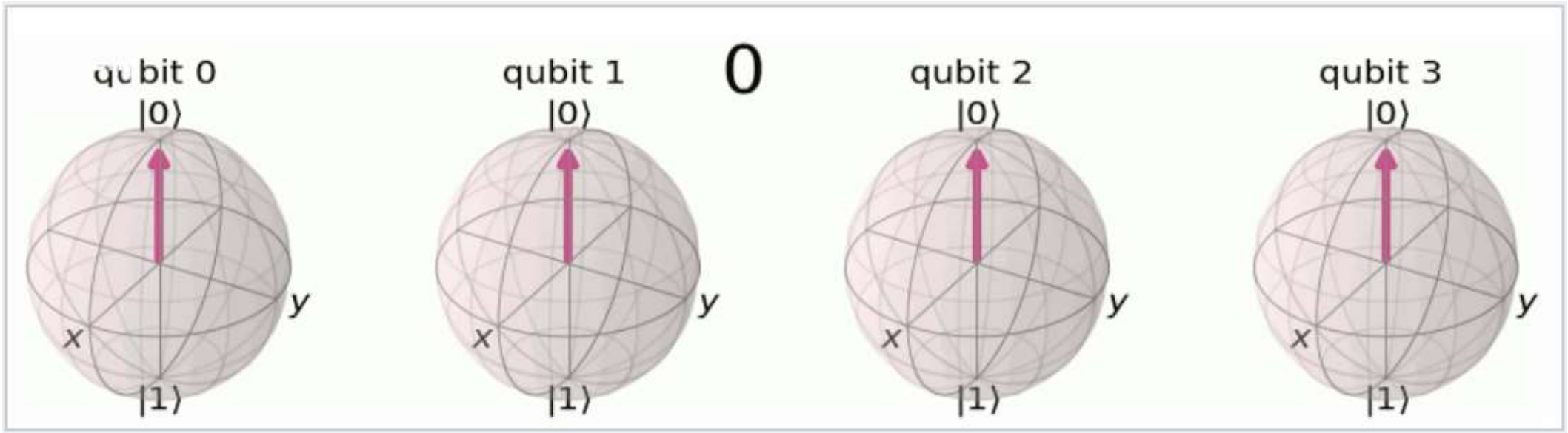


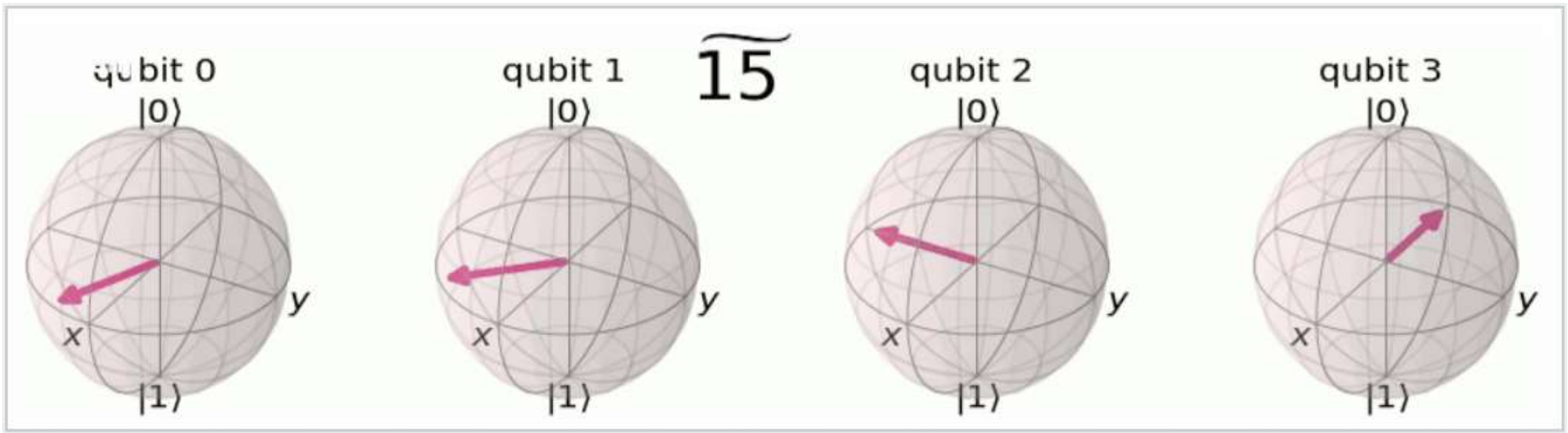
In the *quantum* Fourier transform, we do a DFT on the *amplitudes* of a quantum state:

$$\sum_j \alpha_j |j\rangle \rightarrow \sum_k \tilde{\alpha}_k |k\rangle, \quad \text{where} \quad \tilde{\alpha}_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k/N} \alpha_j.$$

The question is: can we actually carry out this transform physically? This would be possible if there were a unitary operator $\hat{F}$ which transformed a state into its DFT:

$$|\tilde{\psi}\rangle = \hat{F}|\psi\rangle, \quad \hat{F}^\dagger \hat{F} = \hat{I}.$$


qubit 0
|0⟩
|1⟩
x
y
0
qubit 1
|0⟩
|1⟩
x
y
qubit 2
|0⟩
|1⟩
x
y
qubit 3
|0⟩
|1⟩
x
y


qubit 0
|0⟩
|1⟩
x
y
$\widetilde{15}$
qubit 1
|0⟩
|1⟩
x
y
qubit 2
|0⟩
|1⟩
x
y
qubit 3
|0⟩
|1⟩
x
y

The Fourier Basis

- The Fourier transform lets us define a new basis: $|\tilde{x}\rangle = \hat{F}|x\rangle$, where $\{|x\rangle\}$ is the usual computational basis. This basis has a number of interesting properties.
- Every vector $|\tilde{x}\rangle$ is an equally weighted superposition of all the computational basis states:

$$\begin{aligned} |\langle\tilde{x}|y\rangle|^2 &= \langle y|\tilde{x}\rangle\langle\tilde{x}|y\rangle = \langle y|\hat{F}|x\rangle\langle x|\hat{F}^\dagger|y\rangle \\ &= \frac{e^{2\pi ixy/N}}{\sqrt{N}}\frac{e^{-2\pi ixy/N}}{\sqrt{N}} = \frac{1}{N}. \end{aligned}$$

- So if we think of the states $|x\rangle$ as being somehow the most "classical," then the states $|\tilde{x}\rangle$ are somehow as "unclassical" as possible.

Quantum Fourier transform

$$F_N = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)^2} \end{bmatrix}$$

where $\omega = e^{2\pi i/N}$ (for n qubits, $N = 2^n$)

This is unitary and $F_2 = H$, the Hadamard transform

This generalization of H is an important component of several interesting quantum algorithms …

Examples

Ex. 1

Lets take a look at QFT_2. Because $M = 2$, $\omega = 2^{\pi i} = -1$ Therefore we have

$$QFT_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & \omega \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

As you can see, QFT_2 is simply equal to $H^{\otimes 2}$.

How about QFT_4? The primitive 4th root of unity is i, so that

$$QFT_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

Ex. 2

Find the quantum Fourier transform for $M = 4$ of the functions $|f\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle) = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$; $|g\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, and $|h\rangle = |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$.

The corresponding Fourier transforms are given by:

1. QFT_4 to $|f\rangle$.

$$\left|\hat{f}\right\rangle = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

2. QFT_4 on $|g\rangle$:

$$|\hat{g}\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

1. QFT_M is unitary.

Proof It is well known that an operator is unitary if its columns are orthonormal. Denote the ith and jth columns of QFT_M as F_i and F_j.

Then $F_i = \frac{1}{\sqrt{M}} \begin{pmatrix} 1 \\ \omega^{i*1} \\ \vdots \\ \omega^{i*(M-1)} \end{pmatrix}$ and $F_j = \frac{1}{\sqrt{M}} \begin{pmatrix} 1 \\ \omega^{i*j} \\ \vdots \\ \omega^{j*(M-1)} \end{pmatrix}$. Thus

$$\langle F_i | F_j \rangle = \frac{1}{M} \sum_{n=0}^{M-1} \omega^{ni} \overline{\omega^{nj}} = \frac{1}{M} \sum_{n=0}^{M-1} (\omega^{i-j})^n$$

From here it is easy to see that if $i = j$, $\langle F_i | F_j \rangle = 1$.

For the case $i \neq j$, we will notice that $\frac{1}{M}\sum_{n=0}^{M-1}(\omega^{i-j})^n$ is a geometric series, and expand the sum. Thus

$$\frac{1}{M}\sum_{n=0}^{M-1}(\omega^{i-j})^n = \frac{1}{M}\frac{\omega^{M(i-j)}-1}{\omega^{i-j}-1} = \frac{1}{M}\frac{1-1}{\omega^{i-j}-1} = 0$$

where $\omega^{M(i-j)} = 1$ because ω is an Mth root of unity.

Because the Fourier transform is a unitary operator, we can implement it in a quantum circuit. Thus if $N = 2^n$, we can apply the Fourier transform QFT_N to a n-qubit system.

2. *Linear Shift.* This, property exemplified above, states that a linear shift of a state-vector causes a relative phase shift of its Fourier transform. This is expressed mathematically by saying if $|f(x)\rangle$, $x \in \mathbf{Z}_M$ has Fourier transform $\left|\hat{f}(x)\right\rangle$, then $|f(x+j)\rangle$ has Fourier transform $\left|\hat{f}(x)\right\rangle e^{\frac{2\pi}{M}xj}$. Furthermore, because QFT_M is unitary and $QFT_M QFT_M^\dagger = \mathbb{I}$, the converse is true. A linear phase shift on $|f\rangle$ produces a linear shift in $\left|\hat{f}\right\rangle$.

So if $QFT_N \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{N-1} \end{pmatrix}$, then $QFT_N \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_0 \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \omega\beta_1 \\ \vdots \\ \omega^{N-1}\beta_{N-1} \end{pmatrix}$

and $QFT_N \begin{pmatrix} \alpha_0 \\ \omega\alpha_1 \\ \vdots \\ \omega^{N-1}\alpha_{N-1} \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_0 \end{pmatrix}$.

If you have never seen this property before, it should be shocking. We will not offer a proof of this in general here, but below show this in the example that $N = 4$.

Let $|\Theta\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix}$ and $|\Phi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_0 \end{pmatrix}$. Then

$$\left|\hat{\Theta}\right\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 \\ \alpha_0 + i\alpha_1 - \alpha_2 - i\alpha_3 \\ \alpha_0 - \alpha_1 + \alpha_2 - \alpha_3 \\ \alpha_0 - i\alpha_1 - \alpha_2 + i\alpha_3 \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix}$$

$$\left|\hat{\Phi}\right\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 \\ -i\alpha_0 + \alpha_1 + i\alpha_2 - \alpha_3 \\ -\alpha_0 + \alpha_1 - \alpha_2 + \alpha_3 \\ i\alpha_0 + \alpha_1 - i\alpha_2 - \alpha_3 \end{pmatrix} = \begin{pmatrix} \beta_0 \\ -i\beta_1 \\ -\beta_2 \\ i\beta_3 \end{pmatrix}$$

The important point here is that the only difference between $\left|\hat{\Theta}\right\rangle$ and $\left|\hat{\Phi}\right\rangle$ is a relative phase shift. But does this matter?

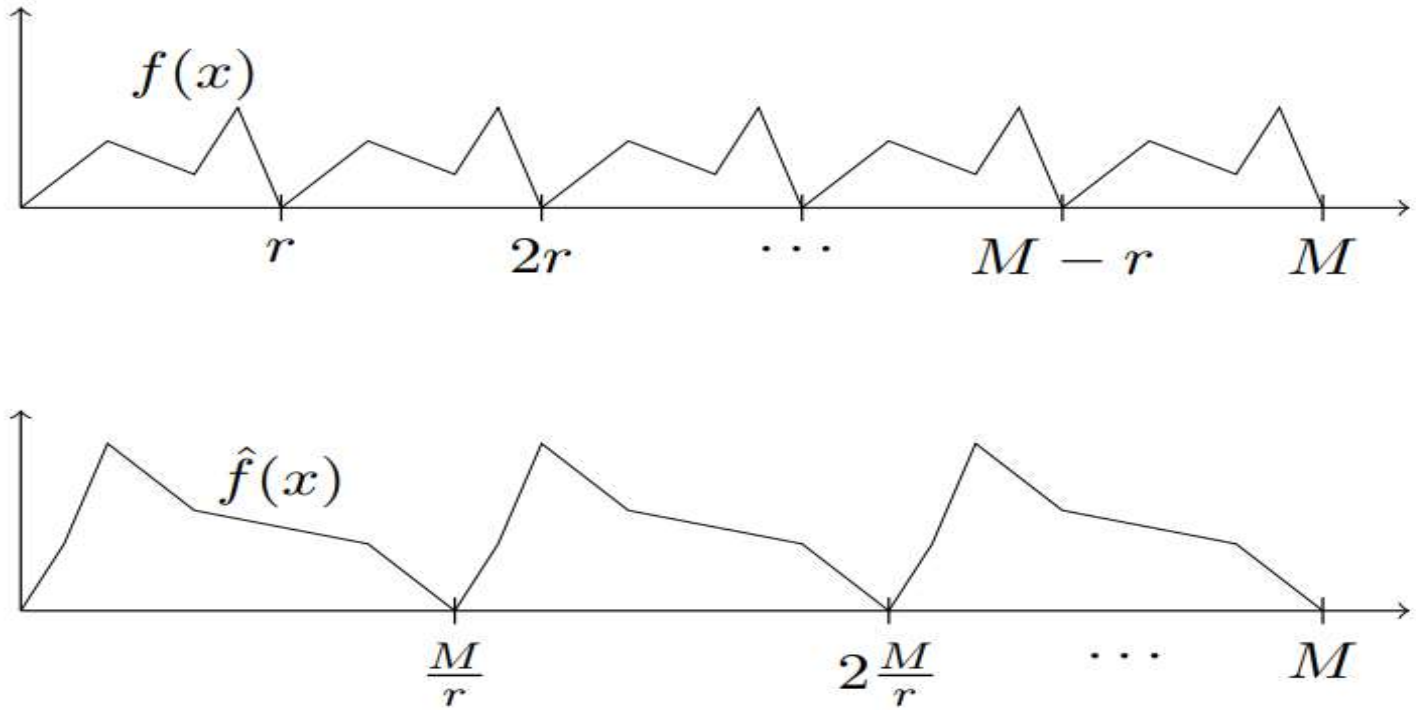
If we are going to measure a state, then the phases don't matter at all, because if the phase is ϕ, $\langle\phi|\phi\rangle = 1$. Therefore the phase of a given state does not effect the probability of measuring that state. However, there is a way we can gather information about the pahses.

We won't be able to tell by measuruing the difference between $\frac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$ and $\frac{1}{2}\begin{pmatrix}1\\i\\-1\\-i\end{pmatrix}$ by making a measurment. However, if we apply QFT, we see that $QFT_4\frac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$ and $QFT_4\frac{1}{2}\begin{pmatrix}1\\i\\-1\\-i\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$. Thus, measuring the Fourier Transform of the states will reveal the relative phases.

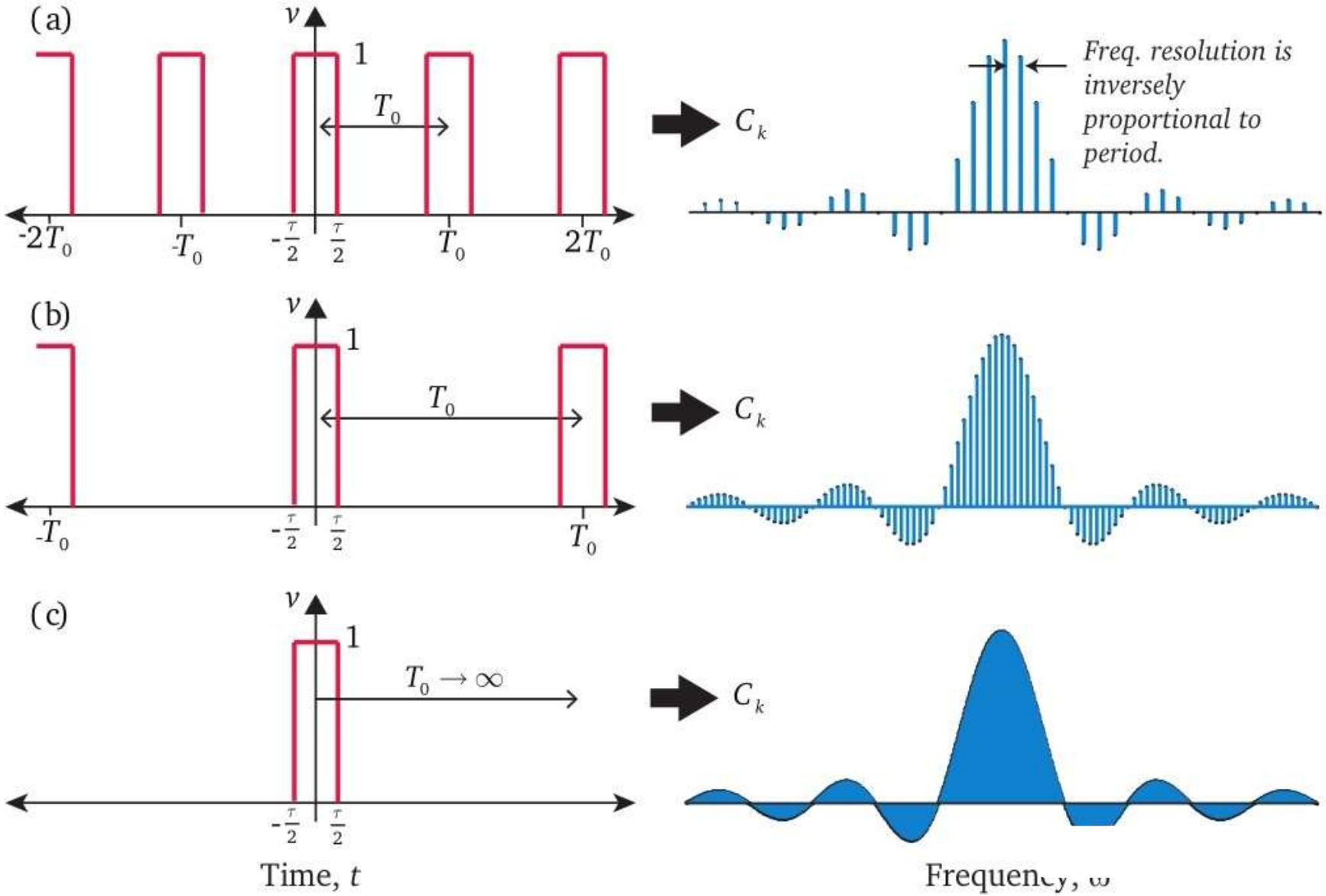
3. *Period/Wavelength Relationship.* Suppose f is periodic with period r, for example

   Then $\hat{f}$ (the Fourier transform of f) is periodic with period M/r. Thus, $\hat{f}$ would look something like below figure.

   If r is the period of f, we can think of M/r as the wavelength of f. If you already have intuition for Fourier transform this should come as no

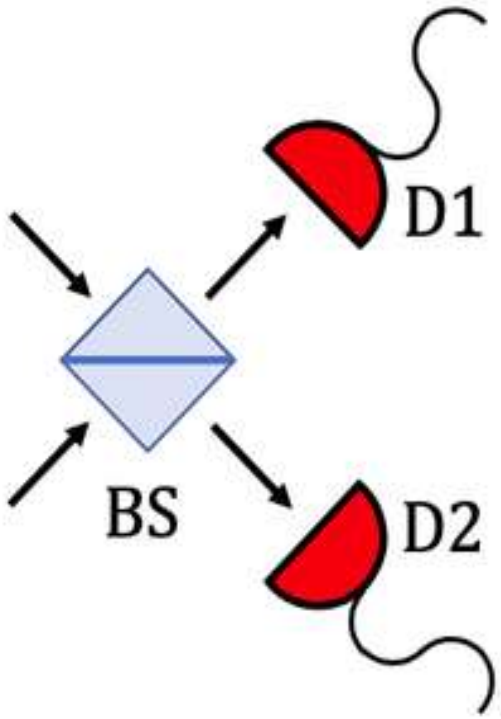


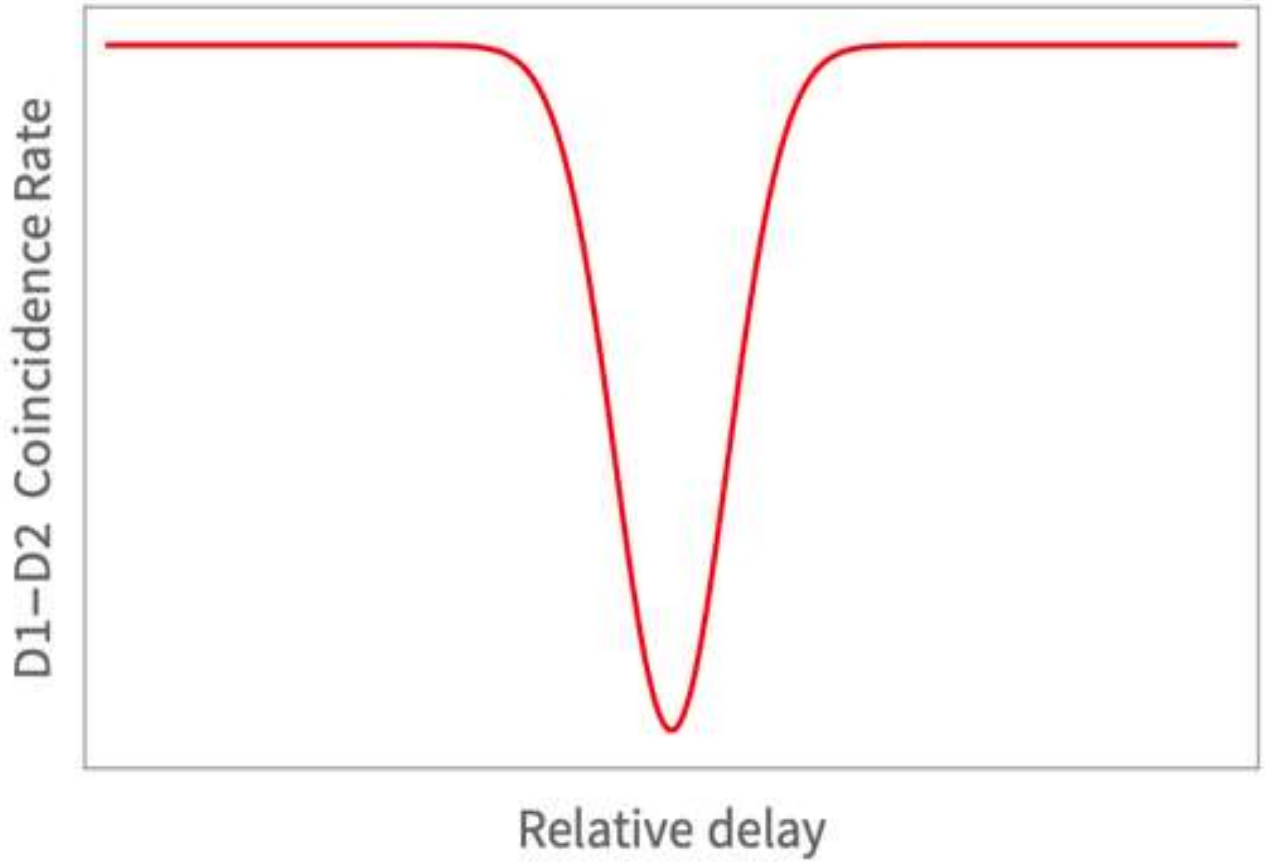
surprise. In general, the wider the range of a function, the sharper the range in the Fourier domain; and vise versa. In example, the fourier transform of a delta function is an even spread, while the transform of an even spread is a delta function.


(a)
v
1
T_0
$-2T_0$
$-T_0$
$-\frac{\tau}{2}$
$\frac{\tau}{2}$
T_0
$2T_0$
C_k
Freq. resolution is inversely proportional to period.
(b)
v
1
T_0
$-T_0$
$-\frac{\tau}{2}$
$\frac{\tau}{2}$
T_0
C_k
(c)
v
1
$T_0 \to \infty$
$-\frac{\tau}{2}$
$\frac{\tau}{2}$
C_k
Time, t
Frequency, ω

Experimental implementation of quantum Fourier transform

Two-dimensional quantum Fourier transform



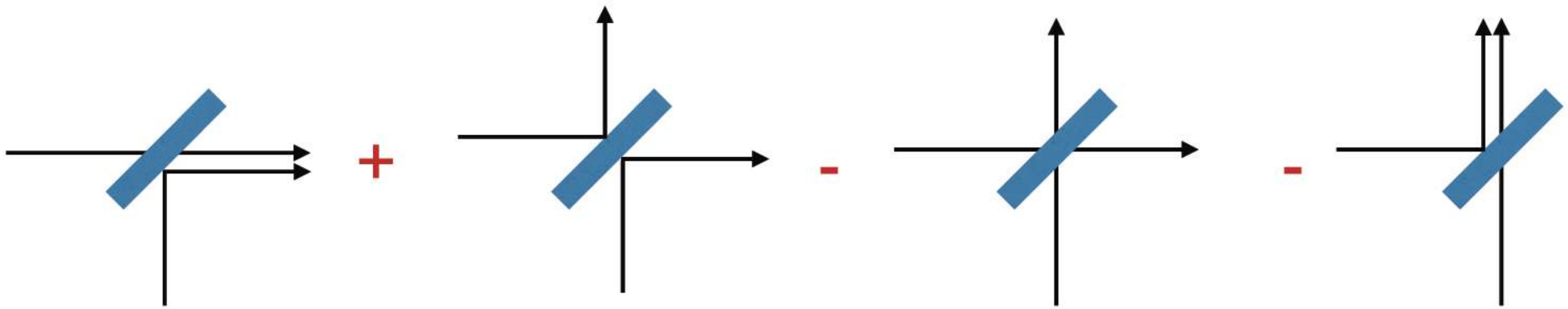


$$\mathbf{H}_2 \triangleq \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

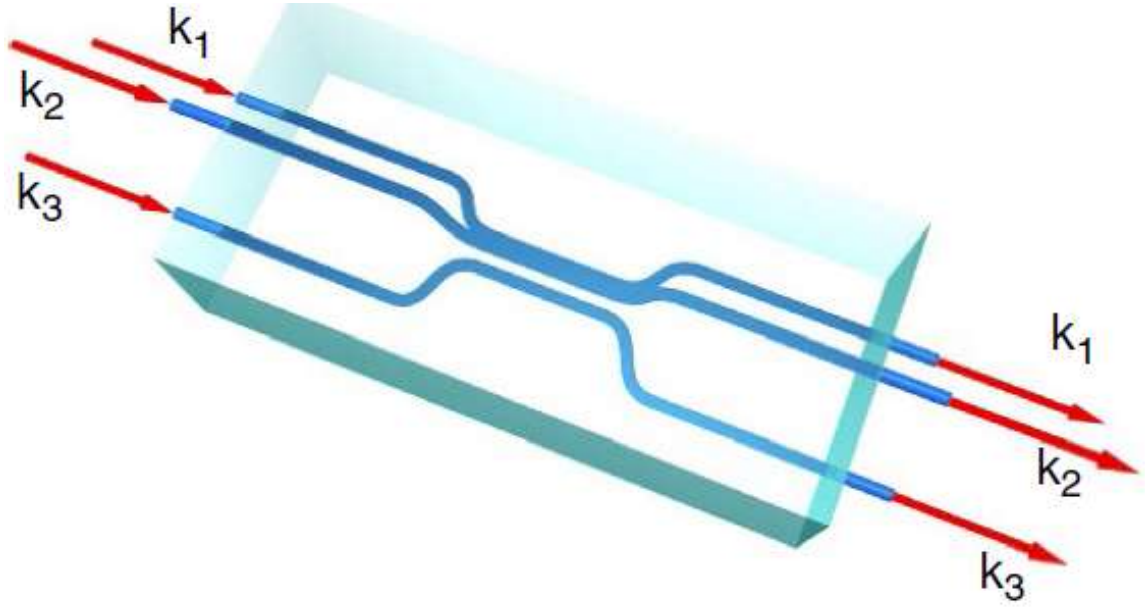
$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix}$$

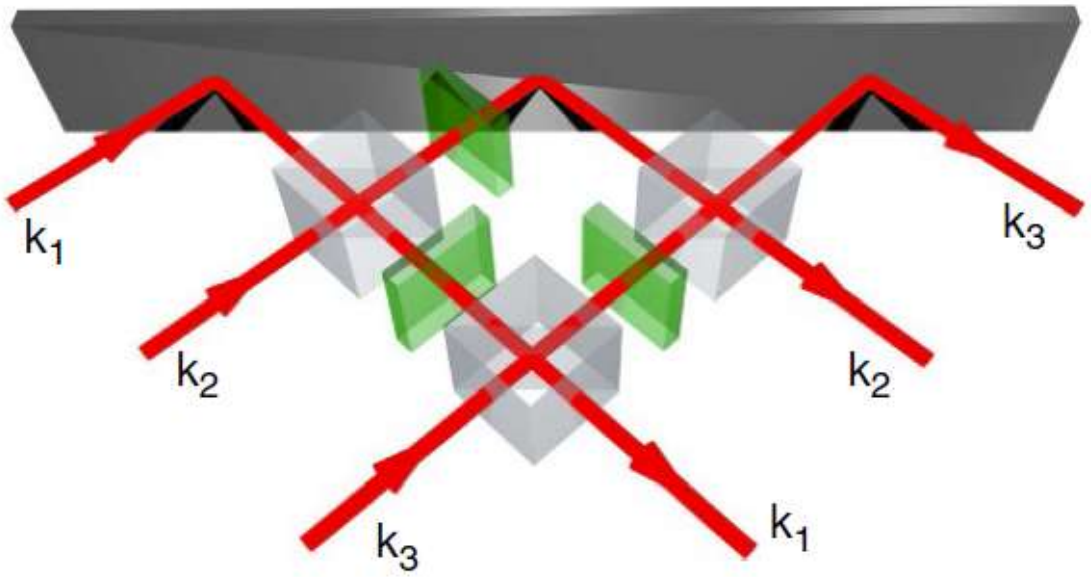
$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix}$$

$$\frac{1}{\sqrt{2}}(|a\rangle+|b\rangle)\otimes\frac{1}{\sqrt{2}}(|a\rangle-|b\rangle)=\frac{1}{2}(|a\rangle|a\rangle+|b\rangle|a\rangle-|a\rangle|b\rangle-|b\rangle|b\rangle)$$

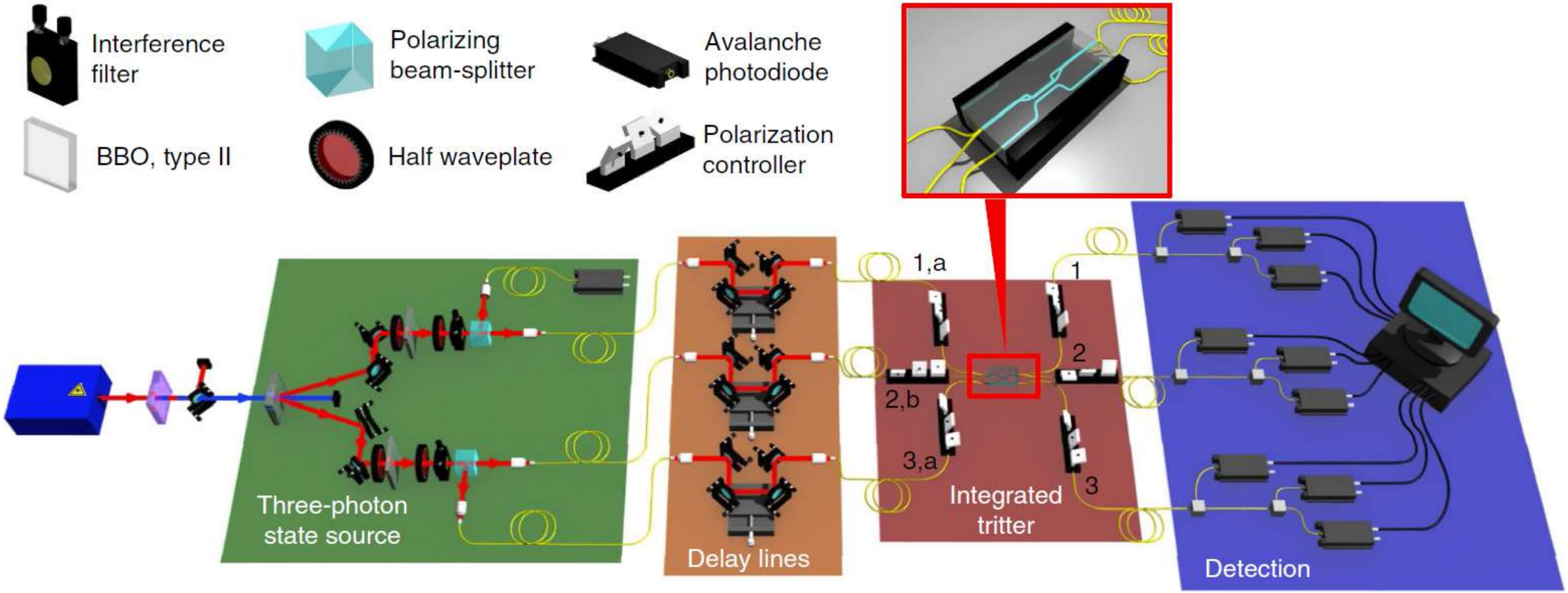


Three-dimensional quantum Fourier transform



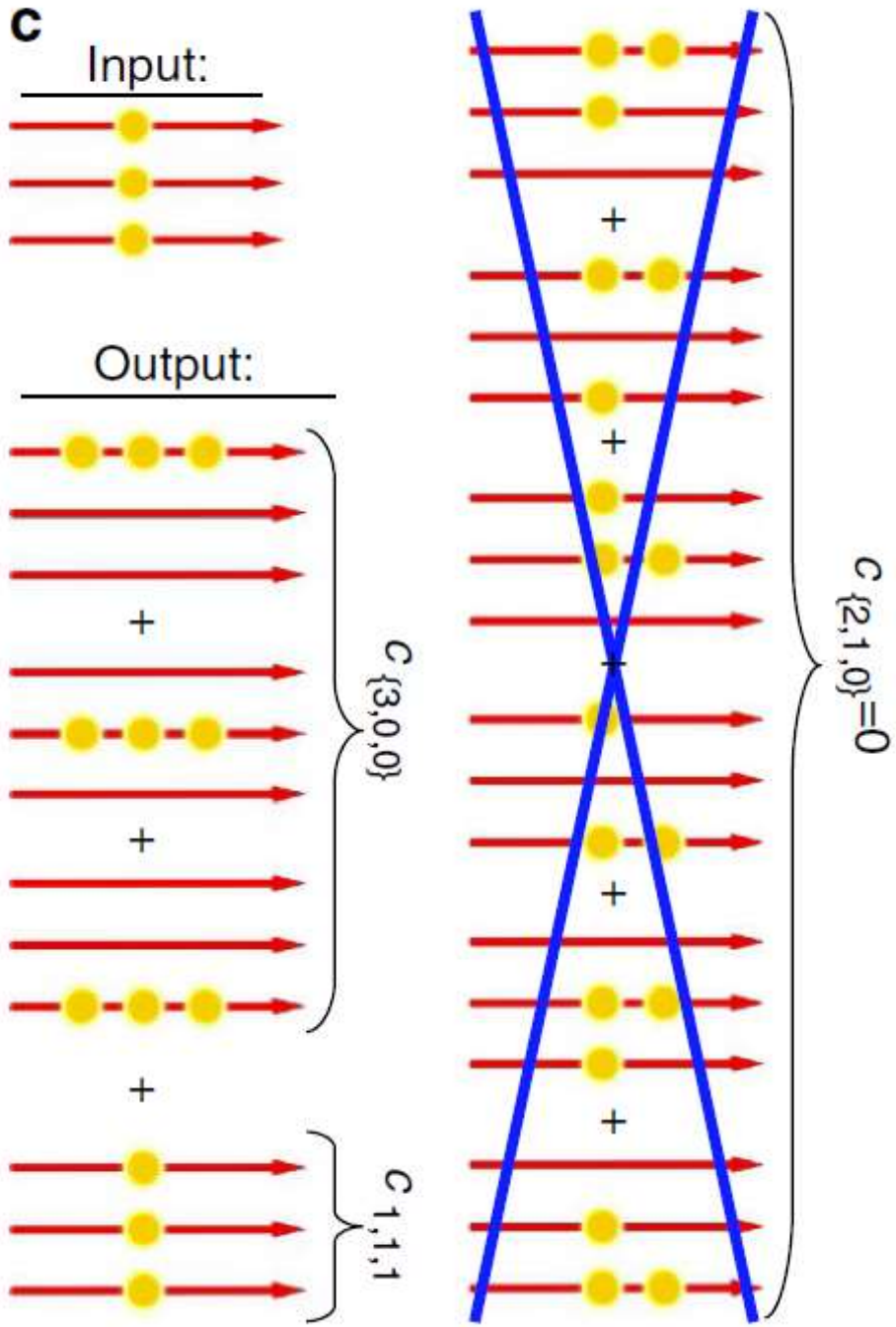


M. C. Tichy, M. Tiersch, F. de Melo, F. Mintert, and A. Buchleitner, Phys. Rev. Lett. 104, 220405 (2010); N. Spagnolo, C. Vitelli, L. Aparo, P. Mataloni, F. Sciarrino, A. Crespi, R. Ramponi, and R. Osellame, Nat. Commun. 4, 1606 (2013).


Interference filter
Polarizing beam-splitter
Avalanche photodiode
BBO, type II
Half waveplate
Polarization controller
1,a
1
2
2,b
3,a
3
Three-photon state source
Delay lines
Integrated tritter
Detection

$$\mathcal{U}^t = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & e^{i2\pi/3} & e^{i4\pi/3} \\ 1 & e^{i4\pi/3} & e^{i8\pi/3} \end{pmatrix}$$

$$|111\rangle \rightarrow \frac{\sqrt{2}}{3}(|300\rangle + |030\rangle + |003\rangle) - \frac{1}{\sqrt{3}}|111\rangle,$$



$$\frac{1}{\sqrt{3}}\begin{bmatrix}1 & 1 & 1\\ 1 & e^{i2\pi/3} & e^{i4\pi/3}\\ 1 & e^{i4\pi/3} & e^{i8\pi/3}\end{bmatrix}\begin{bmatrix}1\\0\\0\end{bmatrix}=\frac{1}{\sqrt{3}}\begin{bmatrix}1\\1\\1\end{bmatrix}$$

$$\frac{1}{\sqrt{3}}\begin{bmatrix}1 & 1 & 1\\ 1 & e^{i2\pi/3} & e^{i4\pi/3}\\ 1 & e^{i4\pi/3} & e^{i8\pi/3}\end{bmatrix}\begin{bmatrix}0\\1\\0\end{bmatrix}=\frac{1}{\sqrt{3}}\begin{bmatrix}1\\e^{i2\pi/3}\\e^{i4\pi/3}\end{bmatrix}$$

$$\frac{1}{\sqrt{3}}\begin{bmatrix}1 & 1 & 1\\ 1 & e^{i2\pi/3} & e^{i4\pi/3}\\ 1 & e^{i4\pi/3} & e^{i8\pi/3}\end{bmatrix}\begin{bmatrix}0\\0\\1\end{bmatrix}=\frac{1}{\sqrt{3}}\begin{bmatrix}1\\e^{i4\pi/3}\\e^{i8\pi/3}\end{bmatrix}$$

$$\frac{1}{\sqrt{3}}(|a\rangle+|b\rangle+|c\rangle)\otimes\frac{1}{\sqrt{3}}(|a\rangle+e^{i2\pi/3}|b\rangle+e^{i4\pi/3}|c\rangle)\otimes\frac{1}{\sqrt{3}}(|a\rangle+e^{i4\pi/3}|b\rangle+e^{i8\pi/3}|c\rangle)$$

$$=\frac{1}{3\sqrt{3}}(|a\rangle|a\rangle|a\rangle+e^{i4\pi/3}|a\rangle|a\rangle|b\rangle+e^{i8\pi/3}|a\rangle|a\rangle|c\rangle+e^{i2\pi/3}|a\rangle|b\rangle|a\rangle+e^{i6\pi/3}|a\rangle|b\rangle|b\rangle$$

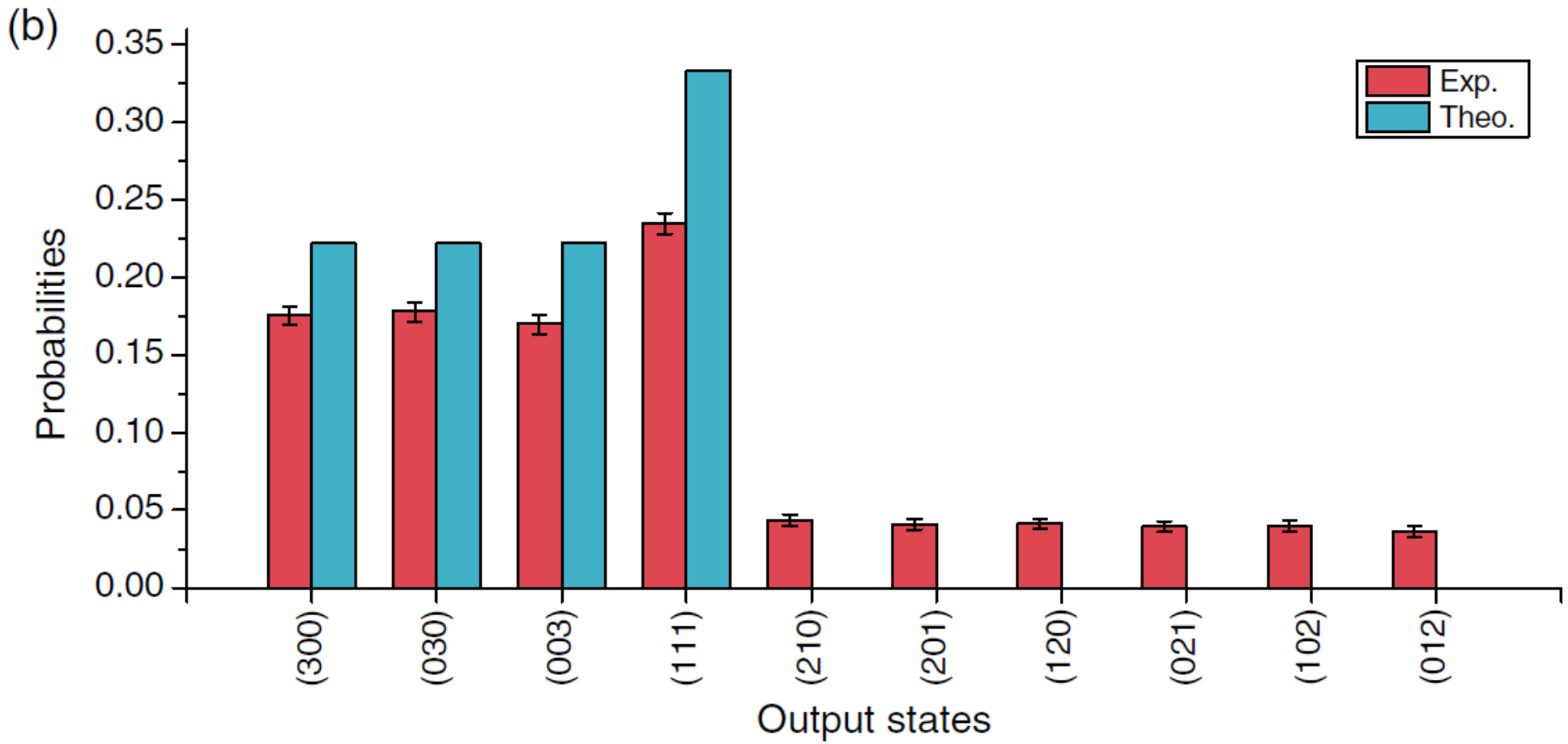
$$+e^{i10\pi/3}|a\rangle|b\rangle|c\rangle+e^{i4\pi/3}|a\rangle|c\rangle|a\rangle+e^{i8\pi/3}|a\rangle|c\rangle|b\rangle+e^{i12\pi/3}|a\rangle|c\rangle|c\rangle+|b\rangle|a\rangle|a\rangle$$

$$+e^{i4\pi/3}|b\rangle|a\rangle|b\rangle+e^{i8\pi/3}|b\rangle|a\rangle|c\rangle+e^{i2\pi/3}|b\rangle|b\rangle|a\rangle+e^{i6\pi/3}|b\rangle|b\rangle|b\rangle+e^{i10\pi/3}|b\rangle|b\rangle|c\rangle$$

$$+e^{i4\pi/3}|b\rangle|c\rangle|a\rangle+e^{i8\pi/3}|b\rangle|c\rangle|b\rangle+e^{i12\pi/3}|b\rangle|c\rangle|c\rangle+|c\rangle|a\rangle|a\rangle+e^{i4\pi/3}|c\rangle|a\rangle|b\rangle$$

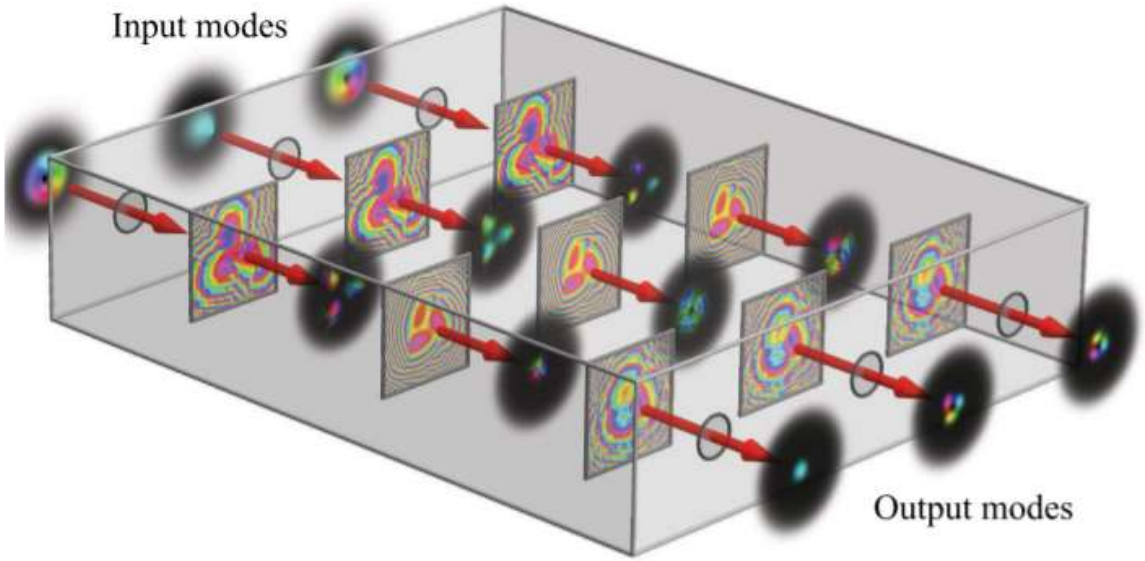
$$+e^{i8\pi/3}|c\rangle|a\rangle|c\rangle+e^{i2\pi/3}|c\rangle|b\rangle|a\rangle+e^{i6\pi/3}|c\rangle|b\rangle|b\rangle+e^{i10\pi/3}|c\rangle|b\rangle|c\rangle+e^{i4\pi/3}|c\rangle|c\rangle|a\rangle$$

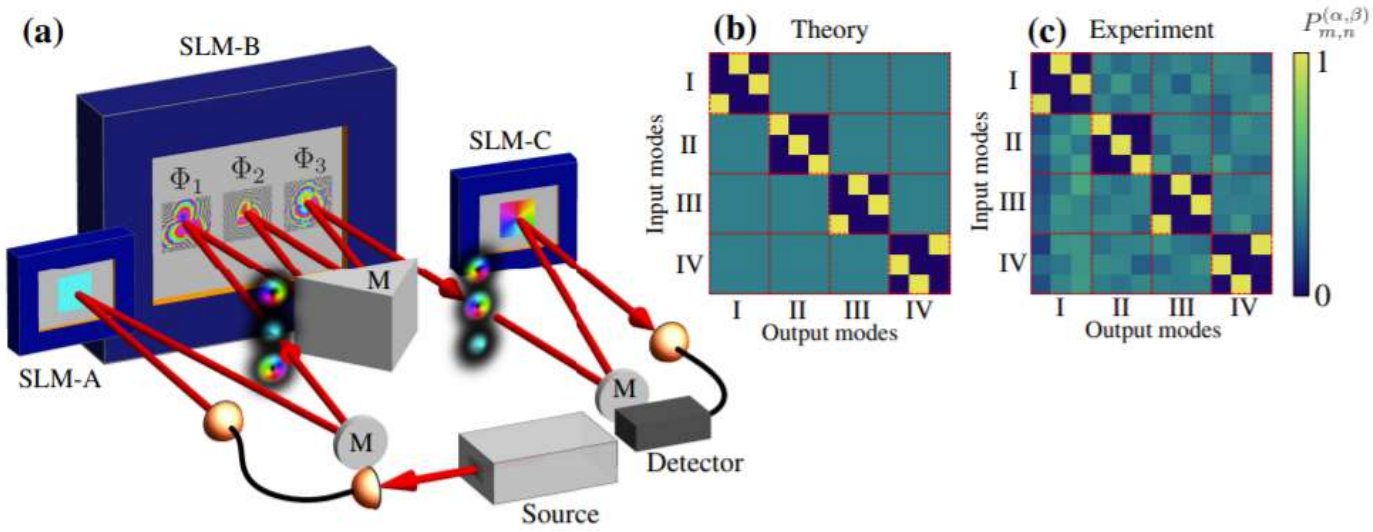
$$+e^{i8\pi/3}|c\rangle|c\rangle|b\rangle+e^{i12\pi/3}|c\rangle|c\rangle|c\rangle)$$



Phys. Rev. Lett. 119, 080502

Higher-dimensional quantum Fourier transform





Optica 7, 98-107 (2020)

Quantum algorithm I: Phase estimation

问题描述：

输入：已知某作用于 n 个量子比特的量子电路 Q （其对应于酉操作 $U \in C^{N\times N}, N=2^n$ ）及量子态 $|\varphi\rangle$ （对应于 U 的特征向量）：

$$U|u\rangle = e^{2\pi i\theta}|u\rangle \tag{1}$$

输出：相位 $\theta \in [0,1)$ 的估计值

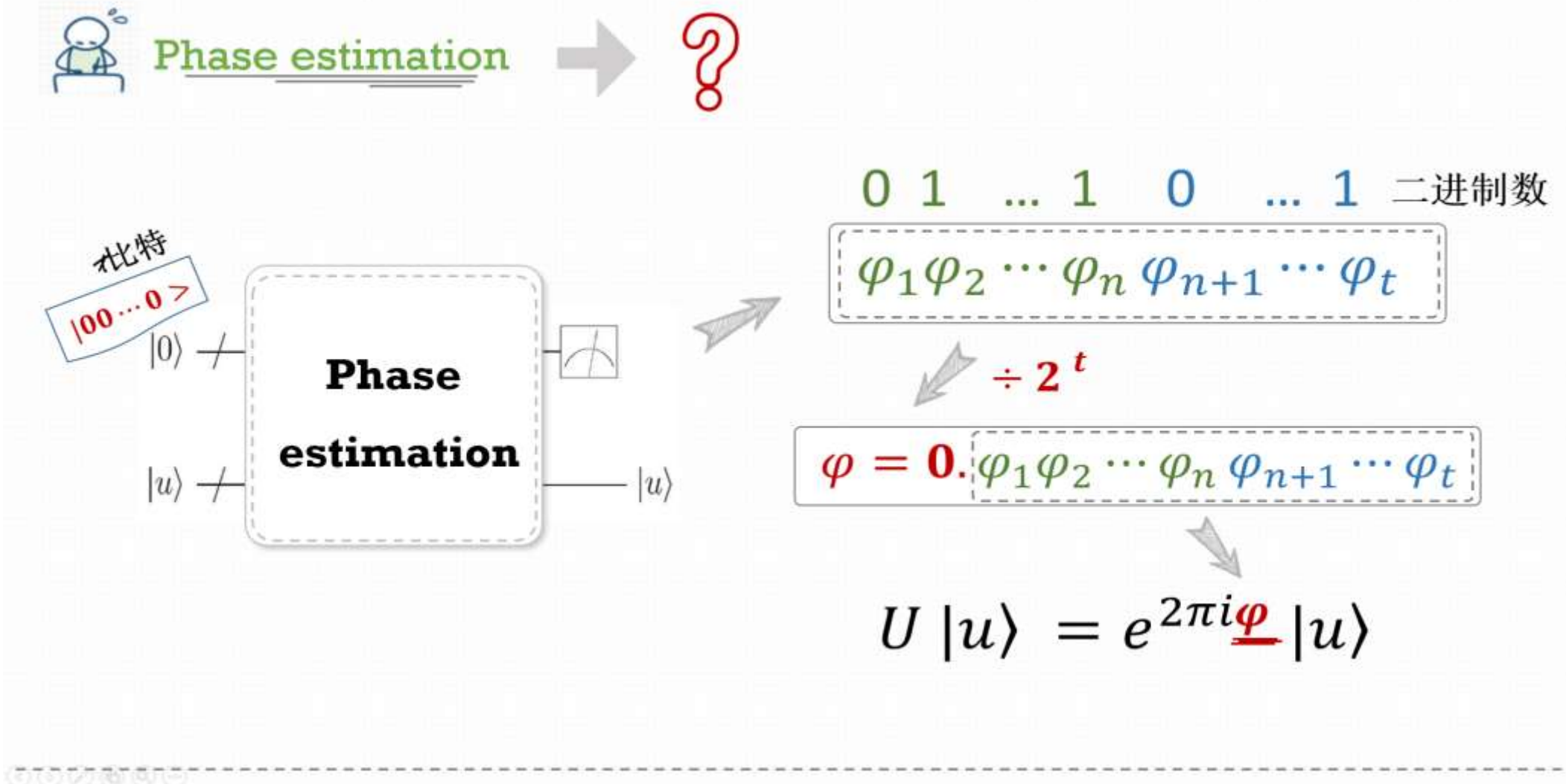
由于 U 为酉矩阵，故有

1. 其特征向量具有完备性及正交性即

$$\{|u_i\rangle\}_{i=1}^{N};\quad \langle u_i|u_j\rangle = 0, i\neq j, i,j=1,\ldots,N$$

2. 其所有特征值的模均为1，故特征值均可表示为

$$\left\{e^{2\pi i\theta_j}\right\}_{j=1}^{N},\quad \theta_j\in[0,1)$$


Phase estimation
0 1 … 1 0 … 1 二进制数
$\varphi_1\varphi_2\cdots\varphi_n\,\varphi_{n+1}\cdots\varphi_t$
$\div 2^t$
$\varphi = 0.\varphi_1\varphi_2\cdots\varphi_n\,\varphi_{n+1}\cdots\varphi_t$
$U\,|u\rangle = e^{2\pi i\varphi}|u\rangle$
n比特
$|00\cdots0\rangle$
$|0\rangle$
$|u\rangle$
Phase estimation
$|u\rangle$

Initial state: $|0\rangle|u\rangle$

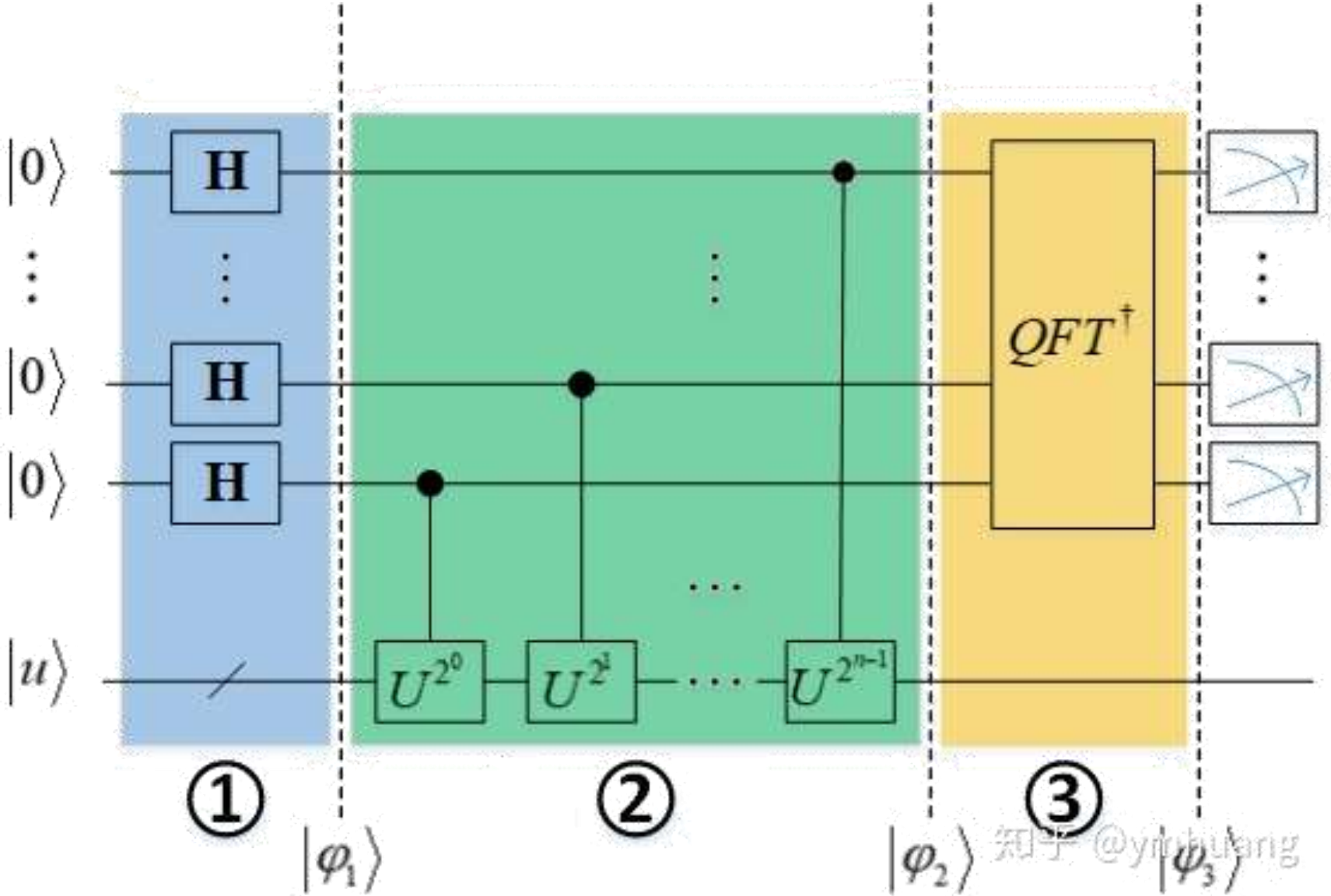
Hadamard operator: $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|u\rangle$

Black box: $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle U^j |u\rangle$

$= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i j \varphi_u} |j\rangle|u\rangle$

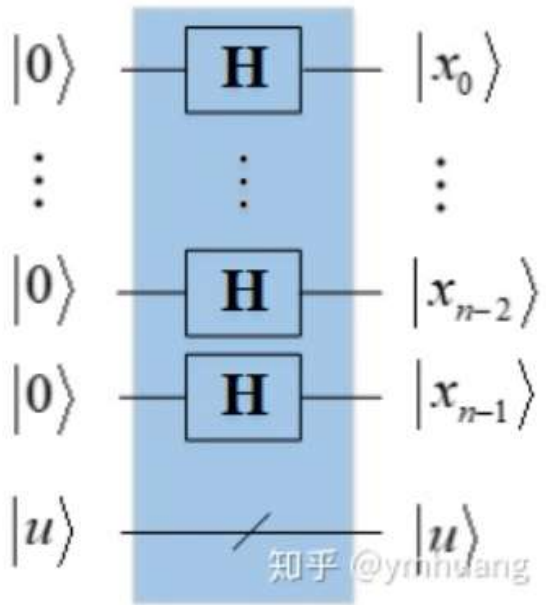
$\rightarrow |\tilde{\varphi}_u\rangle|u\rangle$

Inverse Fourier transform: $\rightarrow \tilde{\varphi}_u$


$|0\rangle$
$|0\rangle$
$|0\rangle$
$|u\rangle$
H
H
H
U^{2^0}
U^{2^1}
$U^{2^{n-1}}$
$QFT^{\dagger}$
①
②
③
$|\varphi_1\rangle$
$|\varphi_2\rangle$
$|\varphi_3\rangle$

第一部分

该部分的输入有两个，一个为 $|0\rangle^{\otimes n}$ 的量子寄存器1和 $|u\rangle$ 的量子寄存器2。该部分目的为准备叠加态，为之后存储相位 θ 做准备。**其思想即把 θ 分解成类似二进制的表示，每qubit负责其中一位。最后读取寄存器1得到的二进制串还原出来的即为 θ 。**

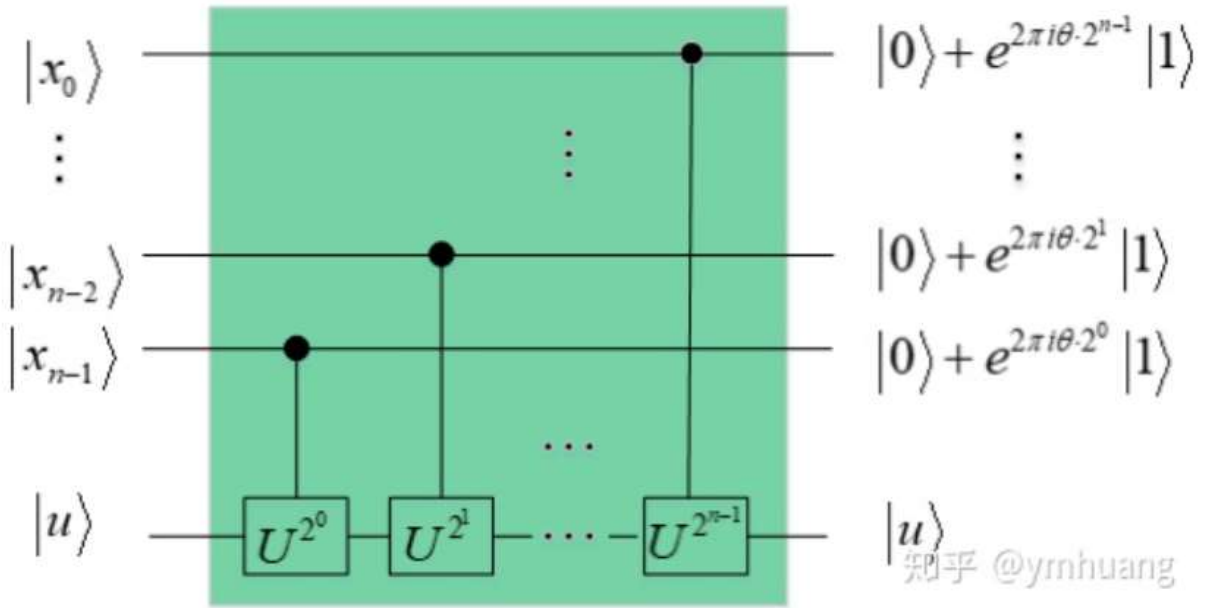


$$|\varphi_1\rangle = \left(H^{\otimes n} \otimes I\right)|0\rangle^{\otimes n}|u\rangle = \frac{1}{\sqrt{2^n}} \sum_{x_0 x_1 \ldots x_{n-1} \in \{0,1\}^n} |x_0 x_1 \ldots x_{n-1}\rangle |u\rangle \quad (2)$$

其中 $x_i \in \{0,1\}$ 。

第二部分

通过对量子寄存器2进行 n 个控制 U^j， $j=2^0,\ldots,2^{n-1}$ 的操作，实现将相位 $e^{2\pi i\theta_j}$ 分别添加到概率幅上。如图所示。其中 $x_i \in \{0,1\}$



因为有分别添加到概率幅上。如图所示

$$U^{2^j}|u\rangle = e^{2\pi i\theta\cdot 2^j}|u\rangle \tag{3}$$

由于使用受控 U 门，所以将 $e^{2\pi i\theta\cdot 2^j}$ 添加到了每个量子比特为 $|1\rangle$ 时的概率幅上。

同时 $\theta \in [0,1)$ ，且可以通过二进制进行展开，得：

$$\theta = \frac{j}{2^n} = 0.\theta_0\theta_1\ldots\theta_{n-1} = \frac{1}{2}\theta_0 + \frac{1}{2^2}\theta_1 + \ldots + \frac{1}{2^n}\theta_{n-1}, j = 1, \ldots, 2^{n-1} \quad (4)$$

其中 $\theta_i \in \{0, 1\}$ 。这样重复使用受控 U 门的好处是，我们的量子态可以表示成

$$U^{2^j} |u\rangle = e^{2\pi i(0.\theta_0\theta_1\ldots\theta_{n-1})\cdot 2^j} |u\rangle = e^{2\pi i 0.\theta_j\theta_{j+1}\ldots\theta_{n-1}} |u\rangle \quad (5)$$

这时我们的整个电路的输出的量子态 $|\varphi_2\rangle$ 为

$$|\varphi_2\rangle = \frac{1}{\sqrt{2^n}} \underbrace{\left(|0\rangle + e^{2\pi i 0.\theta_{n-1}} |1\rangle\right)}_{|x_0\rangle} \underbrace{\left(|0\rangle + e^{2\pi i 0.\theta_{n-2}\theta_{n-1}} |1\rangle\right)}_{|x_1\rangle} \ldots \underbrace{\left(|0\rangle + e^{2\pi i 0.\theta_0\ldots\theta_{n-1}} |1\rangle\right)}_{|x_{n-1}\rangle} |u\rangle \quad (6)$$

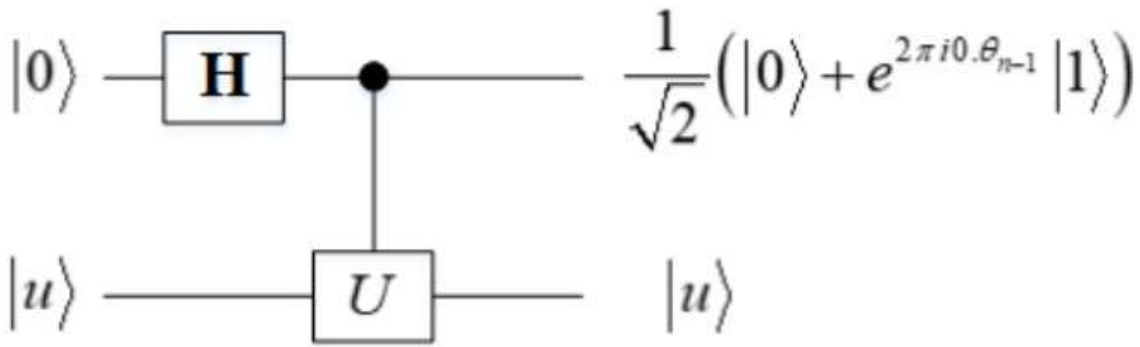
令 $\phi_i = 0.\theta_{n-i+1}..\theta_{n-1}$ ，则有

$$|\varphi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=1, x_0, \ldots, x_{n-1} \in \{0,1\}^n} e^{2\pi i \langle x, \phi_j \rangle} |x_0, \ldots, x_{n-1}\rangle |u\rangle$$

第三部分

考虑最简单的情况。

当 $n=1$ 时，如以下circuit

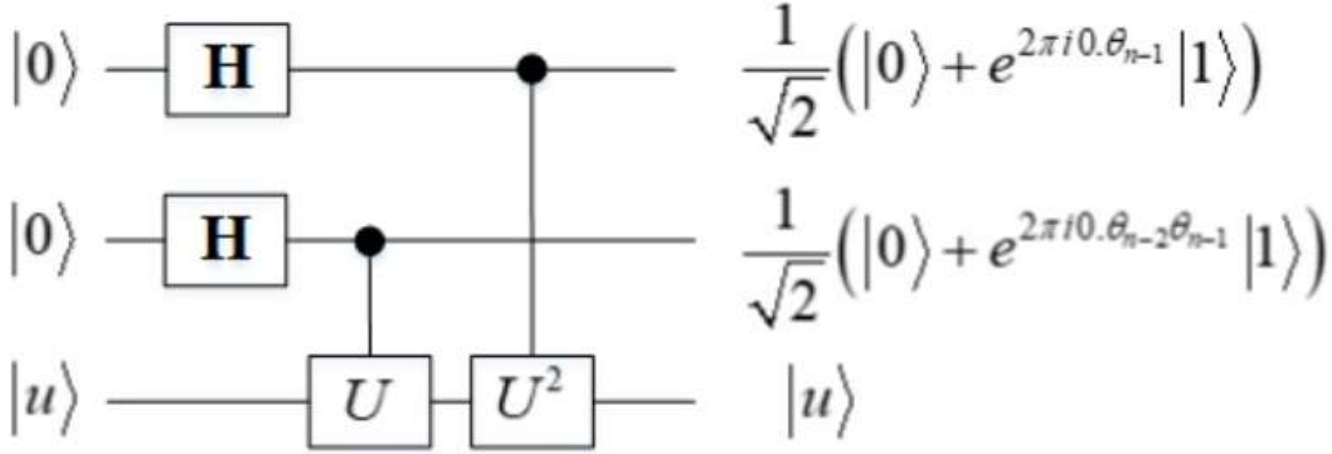


因为 $e^{2\pi i 0.\theta_{n-1}} = \left(e^{\pi i}\right)^{\theta_{n-1}} = (-1)^{\theta_{n-1}}$ ，则有

$$U\left(H \otimes I\right)|0,u\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{\theta_{n-1}}|1\rangle\right)|u\rangle = H|\theta_{n-1}\rangle|u\rangle \qquad (7)$$

这里用到了phase kickback这个trick，也就是将在单量子比特概率幅上的信息，存储到量子态上。这样我们只需要最后对第一个量子比特作用Hardmard门即可将 θ_{n-1} 存储到量子态上。

当 $n=2$ 时，有

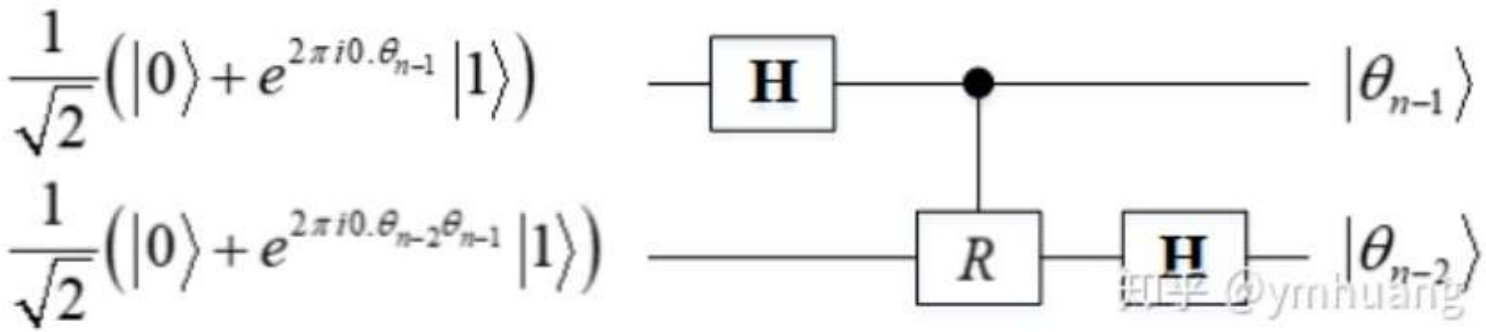


同理，因为

$$e^{2\pi i 0.\theta_{n-2}\theta_{n-1}}=e^{2\pi i\left(\frac{1}{2}\theta_{n-2}+\frac{1}{2^2}\theta_{n-1}\right)}=e^{\pi i\theta_{n-2}}e^{1/2\pi i\theta_{n-1}}=(-1)^{\theta_{n-2}}e^{1/2\pi i\theta_{n-1}}$$

$$\begin{aligned}U^2U\left(H\otimes H\otimes I\right)|0,0,u\rangle&=\frac{1}{\sqrt{2}}\left(|0\rangle+(-1)^{\theta_{n-1}}|1\rangle\right)\left(|0\rangle+(-1)^{\theta_{n-2}}e^{1/2\pi i\theta_{n-1}}|1\rangle\right)|u\rangle\\&=H|\theta_{n-1}\rangle\left(|0\rangle+(-1)^{\theta_{n-2}}e^{1/2\pi i\theta_{n-1}}|1\rangle\right)|u\rangle\end{aligned}\tag{8}$$

很容易看出，为了要提取出 θ_{n-2} 只需要先作用控制旋转门 CR 在作用Hardmard门即可。



其中 旋转门 R 为

$$R = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/4} \end{bmatrix}$$

可见，我们通过 旋转门 R 抵消掉 $e^{1/2\pi i}$ ，使其最终成为 $(-1)^{\theta_{n-1}}$

同理，我们一步一步的对整个寄存器1进行这种操作，即可将相位 θ 存储到量子态上。

通过观察，我们可以发现，这个操作其实就是对寄存器1进行了 $QFT^{\dagger}$ ，即

$$QFT^{\dagger}\,|\varphi_2\rangle = \frac{1}{2^n}\sum_{x,y=0}^{2^n-1} e^{-2\pi xy/2^n}\, e^{2\pi i x\theta}\,|y\rangle$$

Quantum algorithm II: Order-finding algorithm

1. The Problem: Period Finding

Let’s look at the periodic function:

$$f(x) = a^x \bmod N$$

where a and N are positive integers, a is less than N, and they have no common factors. The period, or order (r), is the smallest (non-zero) integer such that:

$$a^r \bmod N = 1$$

We can see an example of this function plotted on the graph below. Note that the lines between points are to help see the periodicity and do not represent the intermediate values between the x-markers.

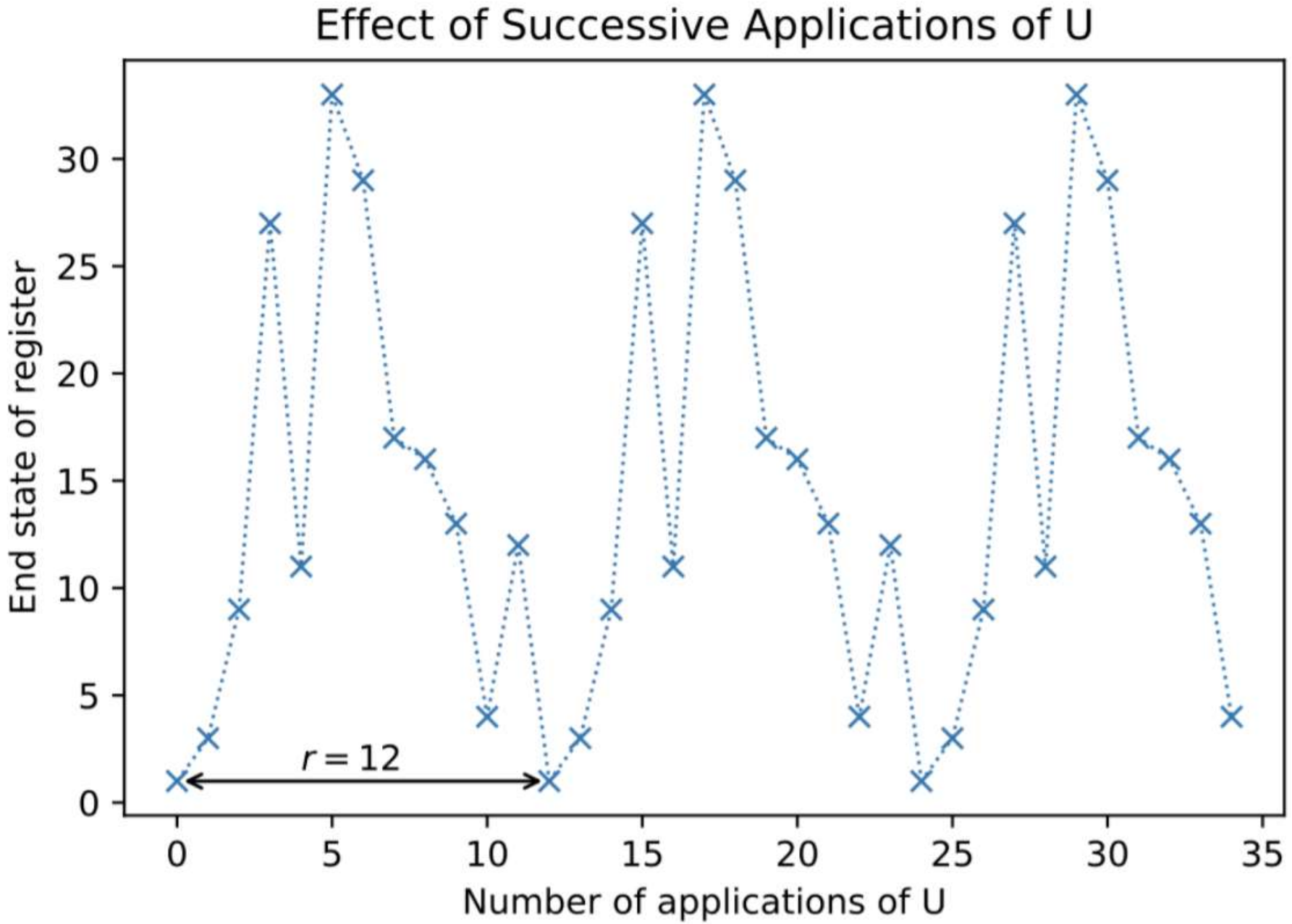
2. The Solution

Shor's solution was to use quantum phase estimation on the unitary operator:

$$U|y\rangle \equiv |ay \bmod N\rangle$$

To see how this is helpful, let's work out what an eigenstate of U might look like. If we started in the state $|1\rangle$, we can see that each successive application of U will multiply the state of our register by $a \pmod N$, and after r applications we will arrive at the state $|1\rangle$ again. For example with $a = 3$ and $N = 35$:

$$\begin{aligned} U|1\rangle &= |3\rangle \\ U^2|1\rangle &= |9\rangle \\ U^3|1\rangle &= |27\rangle \\ &\vdots \\ U^{(r-1)}|1\rangle &= |12\rangle \\ U^r|1\rangle &= |1\rangle \end{aligned}$$


Effect of Successive Applications of U
End state of register
Number of applications of U
r = 12
0
5
10
15
20
25
30
35

So a superposition of the states in this cycle ($|u_0\rangle$) would be an eigenstate of U:

$$|u_0\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |a^k \bmod N\rangle$$

▼ Click to Expand: Example with $a = 3$ and $N = 35$

$$|u_0\rangle = \frac{1}{\sqrt{12}}(|1\rangle + |3\rangle + |9\rangle \cdots + |4\rangle + |12\rangle)$$

$$U|u_0\rangle = \frac{1}{\sqrt{12}}(U|1\rangle + U|3\rangle + U|9\rangle \cdots + U|4\rangle + U|12\rangle)$$

$$= \frac{1}{\sqrt{12}}(|3\rangle + |9\rangle + |27\rangle \cdots + |12\rangle + |1\rangle)$$

$$= |u_0\rangle$$

This eigenstate has an eigenvalue of 1, which isn't very interesting. A more interesting eigenstate could be one in which the phase is different for each of these computational basis states. Specifically, let's look at the case in which the phase of the kth state is proportional to k:

$$|u_1\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i k}{r}} |a^k \bmod N\rangle$$

$$U|u_1\rangle = e^{\frac{2\pi i}{r}} |u_1\rangle$$

▼ Click to Expand: Example with $a = 3$ and $N = 35$

$$|u_1\rangle = \frac{1}{\sqrt{12}}(|1\rangle + e^{-\frac{2\pi i}{12}}|3\rangle + e^{-\frac{4\pi i}{12}}|9\rangle \cdots + e^{-\frac{20\pi i}{12}}|4\rangle + e^{-\frac{22\pi i}{12}}|12\rangle)$$

$$U|u_1\rangle = \frac{1}{\sqrt{12}}(|3\rangle + e^{-\frac{2\pi i}{12}}|9\rangle + e^{-\frac{4\pi i}{12}}|27\rangle \cdots + e^{-\frac{20\pi i}{12}}|12\rangle + e^{-\frac{22\pi i}{12}}|1\rangle)$$

$$U|u_1\rangle = e^{\frac{2\pi i}{12}} \cdot \frac{1}{\sqrt{12}}(e^{\frac{-2\pi i}{12}}|3\rangle + e^{-\frac{4\pi i}{12}}|9\rangle + e^{-\frac{6\pi i}{12}}|27\rangle \cdots + e^{-\frac{22\pi i}{12}}|12\rangle + e^{-\frac{24\pi i}{12}}|1\rangle)$$

$$U|u_1\rangle = e^{\frac{2\pi i}{12}}|u_1\rangle$$

(We can see $r = 12$ appears in the denominator of the phase.)

This is a particularly interesting eigenvalue as it contains r. In fact, r has to be included to make sure the phase differences between the r computational basis states are equal. This is not the only eigenstate with this behaviour; to generalise this further, we can multiply an integer, s, to this phase difference, which will show up in our eigenvalue:

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} |a^k \bmod N\rangle$$

$$U|u_s\rangle = e^{\frac{2\pi i s}{r}} |u_s\rangle$$

▼ Click to Expand: Example with $a = 3$ and $N = 35$

$$|u_s\rangle = \frac{1}{\sqrt{12}}(|1\rangle + e^{-\frac{2\pi is}{12}}|3\rangle + e^{-\frac{4\pi is}{12}}|9\rangle \cdots + e^{-\frac{20\pi is}{12}}|4\rangle + e^{-\frac{22\pi is}{12}}|12\rangle)$$

$$U|u_s\rangle = \frac{1}{\sqrt{12}}(|3\rangle + e^{-\frac{2\pi is}{12}}|9\rangle + e^{-\frac{4\pi is}{12}}|27\rangle \cdots + e^{-\frac{20\pi is}{12}}|12\rangle + e^{-\frac{22\pi is}{12}}|1\rangle)$$

$$U|u_s\rangle = e^{\frac{2\pi is}{12}} \cdot \frac{1}{\sqrt{12}}(e^{-\frac{2\pi is}{12}}|3\rangle + e^{-\frac{4\pi is}{12}}|9\rangle + e^{-\frac{6\pi is}{12}}|27\rangle \cdots + e^{-\frac{22\pi is}{12}}|12\rangle + e^{-\frac{24\pi is}{12}}|1\rangle)$$

$$U|u_s\rangle = e^{\frac{2\pi is}{12}}|u_s\rangle$$

We now have a unique eigenstate for each integer value of s where

$$0 \leq s \leq r - 1.$$

Very conveniently, if we sum up all these eigenstates, the different phases cancel out all computational basis states except $|1\rangle$:

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$$

▼ Click to Expand: Example with $a = 7$ and $N = 15$

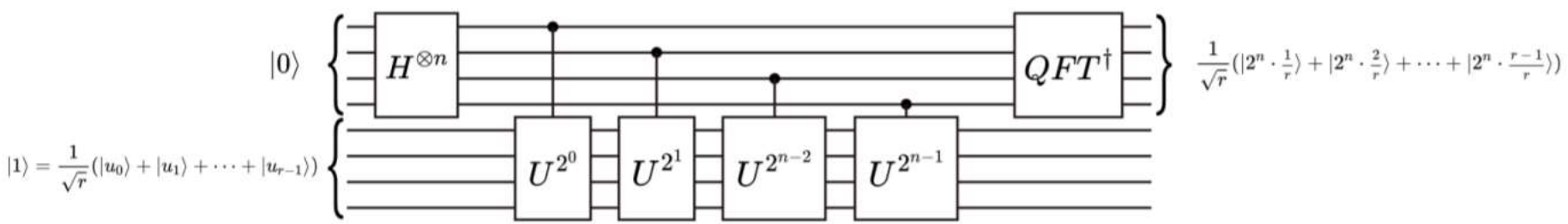
For this, we will look at a smaller example where $a = 7$ and $N = 15$. In this case $r = 4$:

$$\begin{aligned}
\tfrac{1}{2}(\quad |u_0\rangle &= \tfrac{1}{2}(|1\rangle \quad\quad + |7\rangle \quad\quad + |4\rangle \quad\quad + |13\rangle)\dots \\
+|u_1\rangle &= \tfrac{1}{2}(|1\rangle + e^{-\frac{2\pi i}{4}}|7\rangle + e^{-\frac{4\pi i}{4}}|4\rangle + e^{-\frac{6\pi i}{4}}|13\rangle)\dots \\
+|u_2\rangle &= \tfrac{1}{2}(|1\rangle + e^{-\frac{4\pi i}{4}}|7\rangle + e^{-\frac{8\pi i}{4}}|4\rangle + e^{-\frac{12\pi i}{4}}|13\rangle)\dots \\
+|u_3\rangle &= \tfrac{1}{2}(|1\rangle + e^{-\frac{6\pi i}{4}}|7\rangle + e^{-\frac{12\pi i}{4}}|4\rangle + e^{-\frac{18\pi i}{4}}|13\rangle) \quad) = |1\rangle
\end{aligned}$$

Since the computational basis state $|1\rangle$ is a superposition of these eigenstates, which means if we do QPE on U using the state $|1\rangle$, we will measure a phase:

$$\phi = \frac{s}{r}$$

Where s is a random integer between 0 and $r - 1$. We finally use the continued fractions algorithm on ϕ to find r. The circuit diagram looks like this (note that this diagram uses Qiskit's qubit ordering convention):



Procedure:

1. $|0\rangle|1\rangle$ — initial state

2. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|1\rangle$ — create superposition

3. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|x^j \bmod N\rangle$ — apply $U_{x,N}$

$$\approx \frac{1}{\sqrt{r2^t}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} e^{2\pi i s j/r} |j\rangle|u_s\rangle$$

4. $\rightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\widetilde{s/r}\rangle|u_s\rangle$ — apply inverse Fourier transform to first register

5. $\rightarrow \widetilde{s/r}$ — measure first register

6. $\rightarrow r$ — apply continued fractions algorithm