# Lecture 4
# Quantum Fourier Transform and applications : Simon and Shor algorithms

January 29, 2020

# Plan

1. Simon's algorithm and its applications to cryptography
2. The hidden subgroup group problem and the quantum Fourier transform
3. Shor's algorithm
   - reduction to order finding and phase estimation
   - solving the phase estimation problem
   - fast quantum Fourier transform $\mathbf{QFT}_{2^m}$
   - deducing the order from the measurements

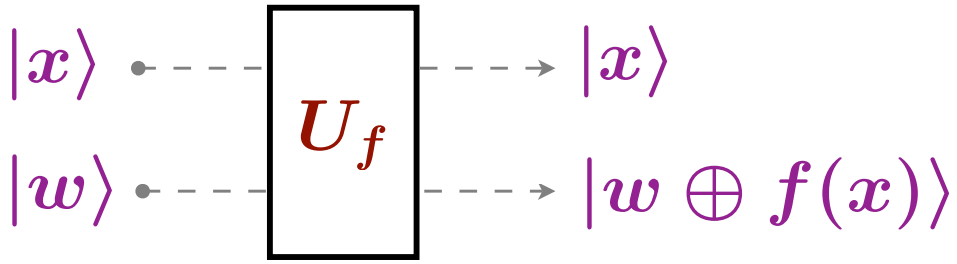
# 1. Simon's algorithm

Input : $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that there exists $s \in \mathbb{F}_2^n$ for which

$$f(x) = f(y) \Leftrightarrow y = x \oplus s$$

Output : $s$

Constraint : blackbox call to $f$



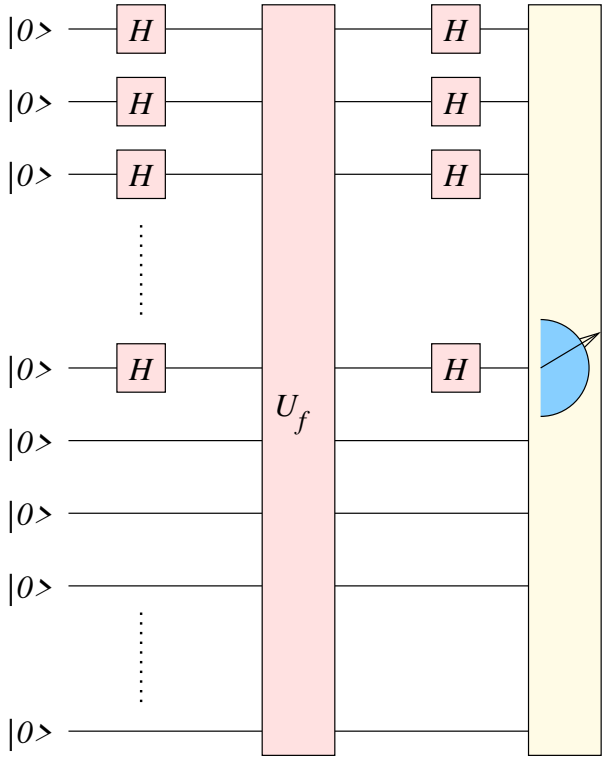
# Query complexity

- Classically $2^{\Omega(n)}$
- Quantumly $O(n)$

## Query complexity

- Classically $O(2^{n/2})$
- Quantumly $O(n)$

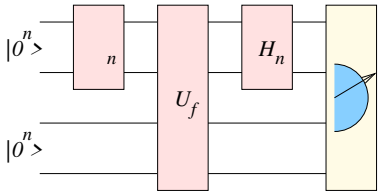
# Simon's algorithm



## Exercise

What is the output of this algorithm ?

# Simon's algorithm




- Initialization: $|0^n\rangle\,|0^n\rangle$
- Parallelization: $\frac{1}{2^{n/2}}\sum_x |x\rangle\,|0^n\rangle$
- Calling $f$: $\frac{1}{2^{n/2}}\sum_{x\in\mathbb{F}_2^n} |x\rangle\,|f(x)\rangle = \frac{1}{2^{n/2}}\sum_{x\in\mathbb{F}_2^n/\langle s\rangle} (|x\rangle + |x\oplus s\rangle)\,|f(x)\rangle$
- Interference:

$$\frac{1}{2^n}\sum_{x\in\mathbb{F}_2^n/\langle s\rangle}\sum_{y\in\mathbb{F}_2^n}(-1)^{x\cdot y}\left(1+(-1)^{y\cdot s}\right)|y\rangle\,|f(x)\rangle$$

$$= \frac{1}{2^{n-1}}\sum_{x\in\mathbb{F}_2^n/\langle s\rangle}\sum_{y:y\cdot s=0}(-1)^{x\cdot y}\,|y\rangle\,|f(x)\rangle$$

- Measure: $|y\rangle\,|f(x)\rangle$ for which $y\cdot s = 0$

## Exercise : one-time pad

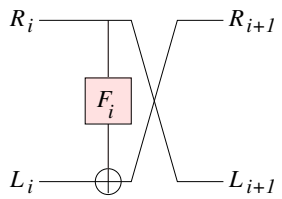
For $K \in \mathbb{F}_2^n$, consider the "one-time pad function"

$$\begin{aligned} E_K : \mathbb{F}_2^n &\to \mathbb{F}_2^n \\ M &\mapsto M \oplus K \end{aligned}$$

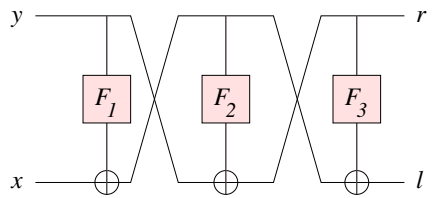
Show that there is a quantum polynomial time algorithm querying $U_{E_K}$ just once that distinguishes $E_K$ from a random permutation $P$ of $\mathbb{F}_2^n$.

## Exercise : Feistel network

Consider the following round function $(L, R) \mapsto (R, L \oplus F_i(R))$ represented by




Let $P$ be the 3-round Feistel cipher given by $P(x, y) = (l, r)$ from 3 round functions $F_1$, $F_2$, $F_3$




1. Express $r = R(x, y)$ in terms of $x$ and $y$
2. Choose two distinct values $\alpha$ and $\beta$ and define $f$ as $f(0, x) = F_2(x \oplus F_1(\alpha))$ and $f_1(x) = F_2(x \oplus F_1(\beta))$. Give a $y$ such that $f(0, x) = f(1, y)$
3. Deduce a polynomial time algorithm that distinguishes $P$ from a random permutation by using only $O(n)$ calls to $U_P$

# 2. The hidden subgroup problem

- Input:
  - a group $G$
  - $f : G \mapsto \mathbb{C}$ a function which is constant and distinct over the cosets of an unknown subgroup $H$ of $G$

$$f(x) = f(y) \Leftrightarrow \exists h \in H : y = xh$$

- Output: $H$

## Exercise : Simon's problem

Explain why Simon's problem is an instance of the HSP problem

## Simon's problem

$$\begin{aligned} G &= \mathbb{F}_2^n \\ H &= \{0, s\} \end{aligned}$$

# Quantum "Supremacy"

- Can be solved in polynomial time $O(\log |G|^a)$ with a quantum computer when $G$ is abelian.
- Factoring and discrete log reduce to this problem.

# Factoring and the hidden subgroup problem

$$
\begin{aligned}
G &= \mathbb{Z} \\
f(x) &= a^x \pmod N \quad a \text{ random in } \mathbb{Z}/N\mathbb{Z} \\
r &= \text{order of } a \text{ (smallest positive integer } r \text{ s.t. } a^r = 1 \pmod N) \\
H &= r\mathbb{Z}
\end{aligned}
$$

# Justification

Assume $r$ is even

$$0 = a^r - 1 \pmod{N} = (a^{r/2} - 1)(a^{r/2} + 1) \pmod{N}$$

$$\begin{aligned} a^{r/2} &\neq 1 \pmod{N} \\ a^{r/2} &\neq -1 \pmod{N} \text{ with prob. } \frac{1}{2} \end{aligned}$$

$\Rightarrow$ GCD$(a^{r/2} - 1, N)$ and GCD$(a^{r/2} + 1, N)$ give a non trivial divisor of $N$.

# Discrete log and hidden subgroup problem

- Input:
  - prime $p$
  - $x$ and $g$ generator of $(\mathbb{Z}/p\mathbb{Z})^*$
- Output: $y$ s.t.

$$x = g^y$$

# Exercise : reducing DLog to HSP

Reduce this problem to HSP

# Reducing DLog to HSP

$$
\begin{aligned}
G &= \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \\
f(a,b) &= g^a x^{-b} \pmod{p} \\
x &= g^y
\end{aligned}
$$

$$
\begin{aligned}
f(a,b) &= g^{a-yb} \pmod{p} \\
f(a_1,b_1) = f(a_2,b_2) &\Leftrightarrow (a_1,b_1) - (a_2,b_2) = \lambda(y,1),\ \lambda \in \mathbb{Z}/(p-1)\mathbb{Z} \\
H &= \langle (y,1) \rangle
\end{aligned}
$$

# The fundamental ingredient : the Fourier transform

- Finite abelian group $G$
- Character group $\hat{G} = \{\chi_g : g \in G\} \cong G$, set of characters = homorphisms from $G$ to the unit complex cercle $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$

$$\begin{aligned} \chi_g : G &\to \mathbb{U} \\ a &\mapsto \chi_g(a), \quad \text{s.t.} \end{aligned}$$

$$\forall a, b \in G \quad \chi_g(a+b) = \chi_g(a)\chi_g(b)$$

Examples:

- $G = \mathbb{F}_2^n = \underbrace{\mathbb{F}_2 \times \mathbb{F}_2 \times \cdots \mathbb{F}_2}_{n \text{ times}}$, $x \cdot y \stackrel{\text{def}}{=} \sum_{i=1}^n x_i y_i$

$$\chi_x(y) = (-1)^{x \cdot y}$$

- $G = \mathbb{Z}_{2^n}$

$$\chi_x(y) = e^{\frac{2i\pi xy}{2^n}}$$

## Fundamental properties

$$\sum_{g\in G}\overline{\chi_1}(g)\chi_2(g)=\begin{cases}|G|, & \text{if } \chi_1=\chi_2\\ 0 & \text{else}\end{cases}\qquad \sum_{\chi\in\hat{G}}\overline{\chi}(g_1)\chi(g_2)=\begin{cases}|G|, & \text{if } g_1=g_2\\ 0 & \text{else}\end{cases}$$

- The matrix $\mathbf{U}=(u_{gg'})_{\substack{g\in G\\ g'\in G}}$ where $u_{gg'}\overset{\text{def}}{=}\frac{1}{\sqrt{|G|}}\chi_{g'}(g)$ is unitary
- It diagonalizes the translation operators $\tau_a$, $a\in G$

$$\begin{aligned}\tau_a:\mathbf{x}\in\mathbb{C}^{|G|} &\to \mathbb{C}^{|G|}\\ (x_g)_{g\in G} &\mapsto (x_{g+a})_{g\in G}\\ \boldsymbol{\chi}_{g'} &\overset{\text{def}}{=} (\chi_{g'}(g))_{g\in G}\\ \tau_a(\boldsymbol{\chi}_{g'}) &= (\chi_{g'}(g+a))_{g\in G}=\underbrace{\chi_g(a)}_{\text{eigenvalue}}\ \underbrace{\boldsymbol{\chi}_{g'}}_{\text{eigenvector}}\end{aligned}$$

# The orthogonal subgroup

**Définition**[**orthogonal subgroup**] For a subgroup $H$ of $G$ we denote by $H^{\perp}$ the orthogonal subgroup defined by

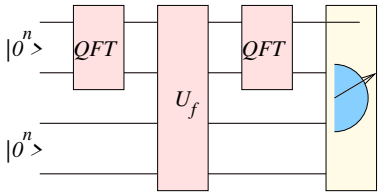
$$H^{\perp} \stackrel{\text{def}}{=} \{g \in G : \chi_g(h) = 1,\ \forall h \in H\}$$

$$\sum_{h \in H} \mathcal{X}_g(h) = \begin{cases} |H|, & \text{if } g \in H^{\perp} \\ 0 & \text{else} \end{cases}$$

# The quantum Fourier transform

| classical Fourier transform | quantum Fourier transform |
|---|---|
| function $f : G \to \mathbb{C}$ | $\lvert\psi\rangle \in \mathbb{C}^{\lvert G\rvert}$ |
| $\mathbf{f} = (f(x))_{x\in G}$ | $\lvert\psi\rangle = \sum_{x\in G} f(x)\lvert x\rangle \quad (\lVert\mathbf{f}\rVert = 1)$ |
| $\hat{f}(g) = \frac{1}{\sqrt{\lvert G\rvert}}\langle \boldsymbol{\chi}_{-g} \lvert f\rangle$ | $\lvert\hat{\psi}\rangle = U\lvert\psi\rangle$ |
| $= \frac{1}{\sqrt{\lvert G\rvert}}\sum_{x\in G}\chi_g(x)f(x)$ | $= \frac{1}{\sqrt{\lvert G\rvert}}\sum_{x,g\in G}\chi_g(x)f(x)\lvert g\rangle$ |
| | $= \sum_{g\in G}\hat{f}(g)\lvert g\rangle$ |

# Generalization of Simon's algorithm




- Initialization: $|0^n\rangle\,|0^n\rangle$
- Parallelization: $\frac{1}{\sqrt{|G|}}\sum_g |g\rangle\,|0^n\rangle$
- Calling $f$: $\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle\,|f(g)\rangle = \frac{1}{\sqrt{|G|}}\sum_{x\in G/H}\sum_{h\in H}|x+h\rangle\,|f(x)\rangle$
- Interference:

$$\frac{1}{|G|}\sum_{x\in G/H}\sum_{g'\in G}\sum_{h\in H}\chi_{g'}(x+h)\,|g'\rangle\,|f(x)\rangle$$

$$= \frac{1}{|G|}\sum_{x\in G/H}\sum_{g'\in G}\chi_{g'}(x)\sum_{h\in H}\chi_{g'}(h)\,|g'\rangle\,|f(x)\rangle$$

$$= \frac{|H|}{|G|}\sum_{x\in G/H}\sum_{g'\in H^\perp}\chi_{g'}(x)\,|g'\rangle\,|f(x)\rangle$$

- Measure: $|g'\rangle\,|f(x)\rangle$ for which $g'\in H^\perp$

# Fast Quantum Fourier Transform

- For $G = \mathbb{F}_2^n$, Fourier transform in $O(n)$ : perform $\mathbf{H}^{\otimes n}$

**Theorem 1.** $\mathbf{QFT}_{\mathbb{Z}_N}$ *can be implemented by a quantum circuit of size* $O(\log N)^2$ *when the divisors of* $N$ *are bounded*

**Theorem 2.** $\mathbf{QFT}_{\mathbb{Z}_N}$ *can be implemented by a quantum circuit of size* $O(\log N)^3$ *in general*

**Theorem 3.** $\mathbf{QFT}_{\mathbb{Z}_N}$ *can be implemented with an accuracy* $\varepsilon$ *with a quantum circuit of size* $O\left(\log N \log\left(\frac{\log N}{\varepsilon} + \log^2(1/\varepsilon)\right)\right)$

# 3. Shor's algorithm

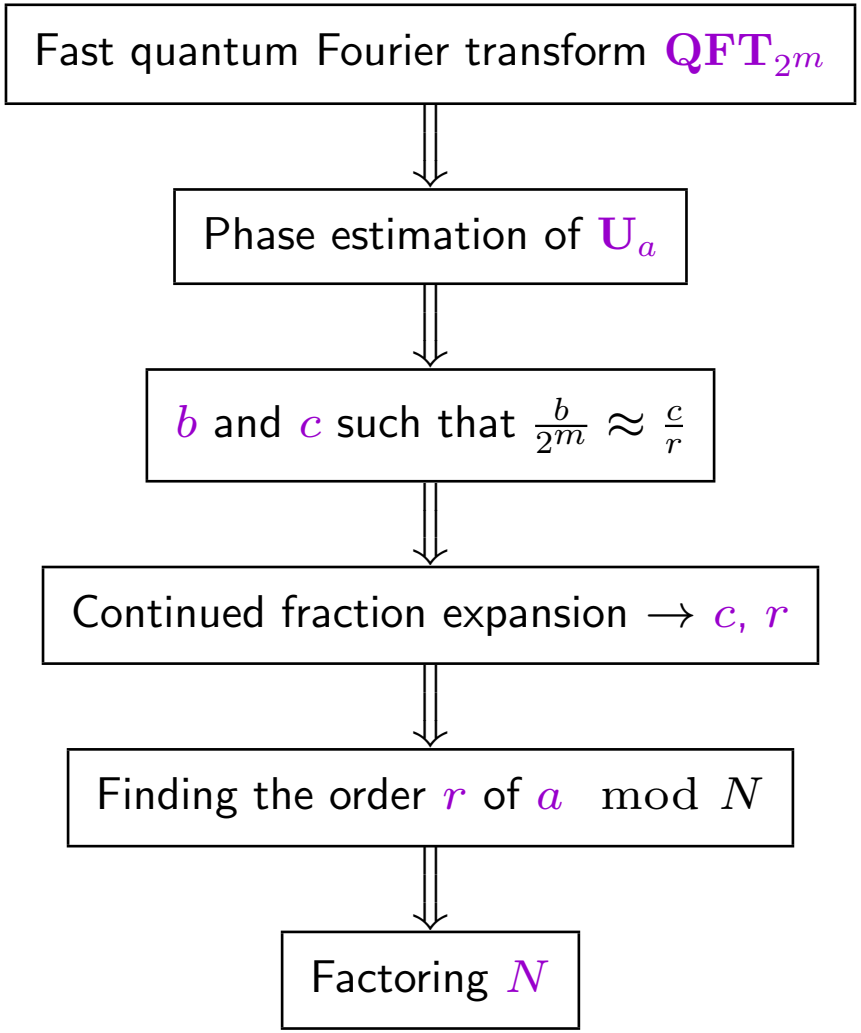
- Factoring $N$: reduction to order finding

**Problem 1. [Order finding]**
*Input:* $a, N$ *with* $a \wedge N = 1$
*Output:* *the smallest* $r \in \mathbb{N}^*$ *such that* $a^r = 1 \pmod N$

**Algorithm**

1. check whether $a \wedge N = 1$
2. compute the order $r$ of $a \pmod N$
3. start again with another $a$ if $r$ odd or $a^{r/2} = -1 \pmod N$
4. return $\mathbf{gcd}(a^{r/2} \pm 1, N)$

# The global picture



# The phase estimation problem

**Problem 2. [phase estimation]**

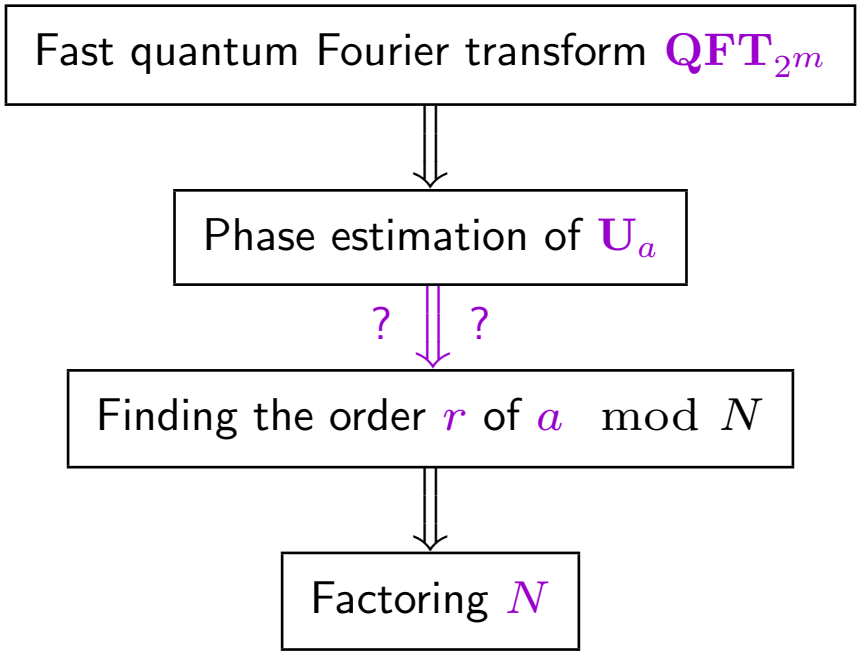
*Input:* *a quantum circuit $Q$ performing a unitary $\mathbf{U}$ along with a quantum eigenstate of $\mathbf{U}$:*

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

*Output:* *an approximation to $\theta$ with precision $\varepsilon$*

- In general approximation complexity has a multiplicative overhead of $O(\frac{1}{\varepsilon})$
- For certain $\mathbf{U}$ much faster approximation can be performed (applies to factoring)

# The global picture

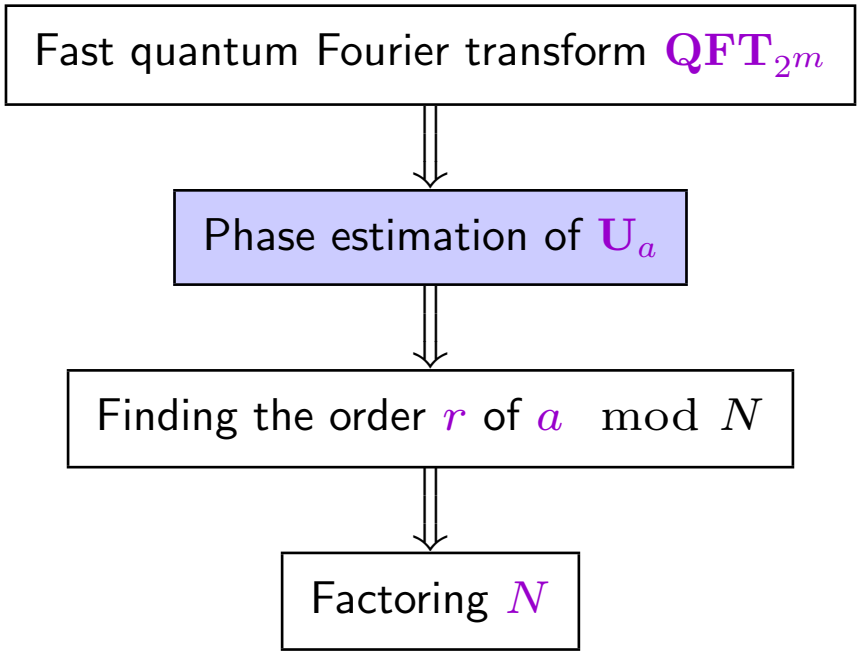


# Reduction to the phase estimation problem

$$\mathbf{U}_a : |x\rangle \mapsto |ax \mod N\rangle$$

1. The space $V$ generated by $\{|1\rangle, |a\rangle, \cdots, |a^{r-1}\rangle\}$ is invariant by $\mathbf{U}_a$
2. The restriction of $\mathbf{U}$ to $V$ has
   - eigenvalues $\lambda_k = e^{2i\pi k/r}$
   - eigenvectors $|\phi_k\rangle = \frac{1}{\sqrt{r}} \sum_{m=0}^{r-1} e^{-2\pi ikm/r} |a^m\rangle$

# The global picture



# $\Lambda_m(\mathbf{U})$

- $\mathbf{U}$ unitary acting on $n$ qubits and $m \in \mathbb{N}^*$ $\Lambda_m(\mathbf{U})$ unitary acting on $m+n$ qubits as

$$\Lambda_m(\mathbf{U}) \left|k\right\rangle \left|\psi\right\rangle = \left|k\right\rangle \left(\mathbf{U}^k \left|\psi\right\rangle\right)$$

$$\mathbf{U}_a : \left|x\right\rangle \mapsto \left|ax \mod N\right\rangle$$

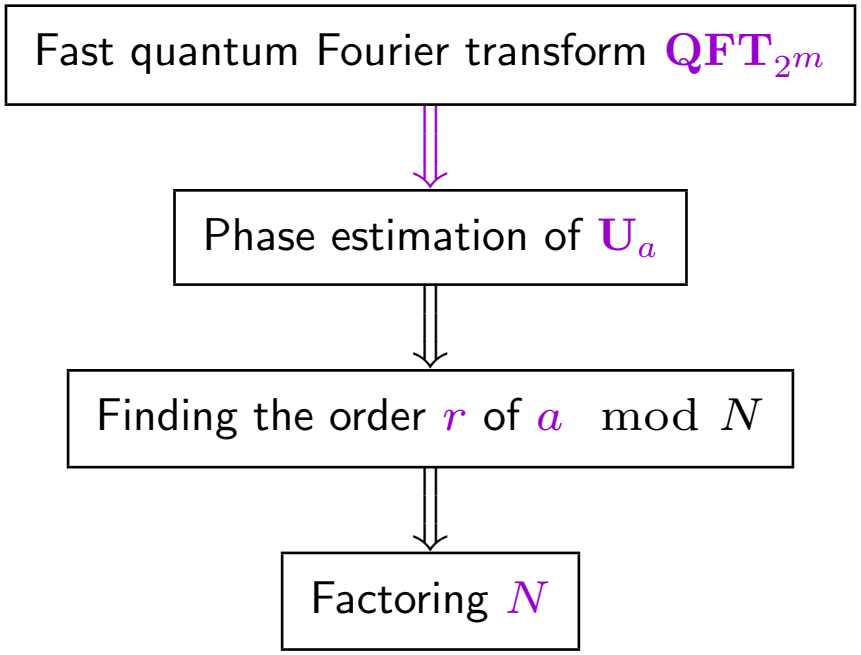
- $\Lambda_m(\mathbf{U}_a)$ can be implemented with $O(mn^2)$ gates using the standard modular exponentiation algorithm, based on a quantum version of a classical reversible circuit performing

$$(x, y) \mapsto (x, a^x y)$$

## Exercise

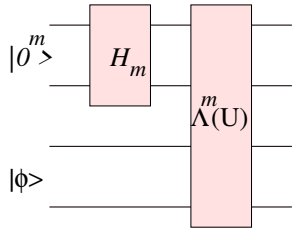
Give a circuit of polynomial complexity performing $\Lambda_m(\mathbf{U})$ involving only one certain c-$\mathbf{U}^j$.

# The global picture



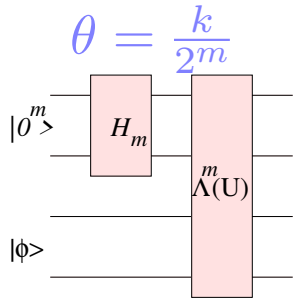
## Exercise : the case when $\theta = \frac{j}{2^m}$

1. Let $|\phi\rangle$ be an eigenvector associated to $\mathbf{U}$ with eigenvalue $e^{\frac{2i\pi k}{2^m}}$ for some $k \in \mathbb{N}$. What is the output of the following circuit ?




2. Add something to this circuit so that after measuring we recover $k$. *Hint:* recall that

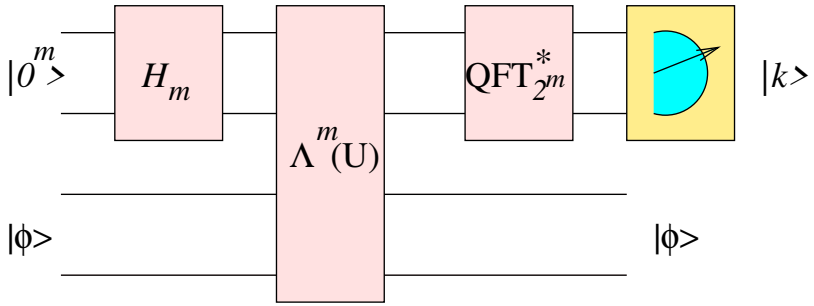
$$\mathbf{QFT}_{2^m} |x\rangle = \frac{1}{\sqrt{2^m}} \sum_{y=0}^{2^m-1} e^{\frac{2i\pi xy}{2^m}} |y\rangle$$



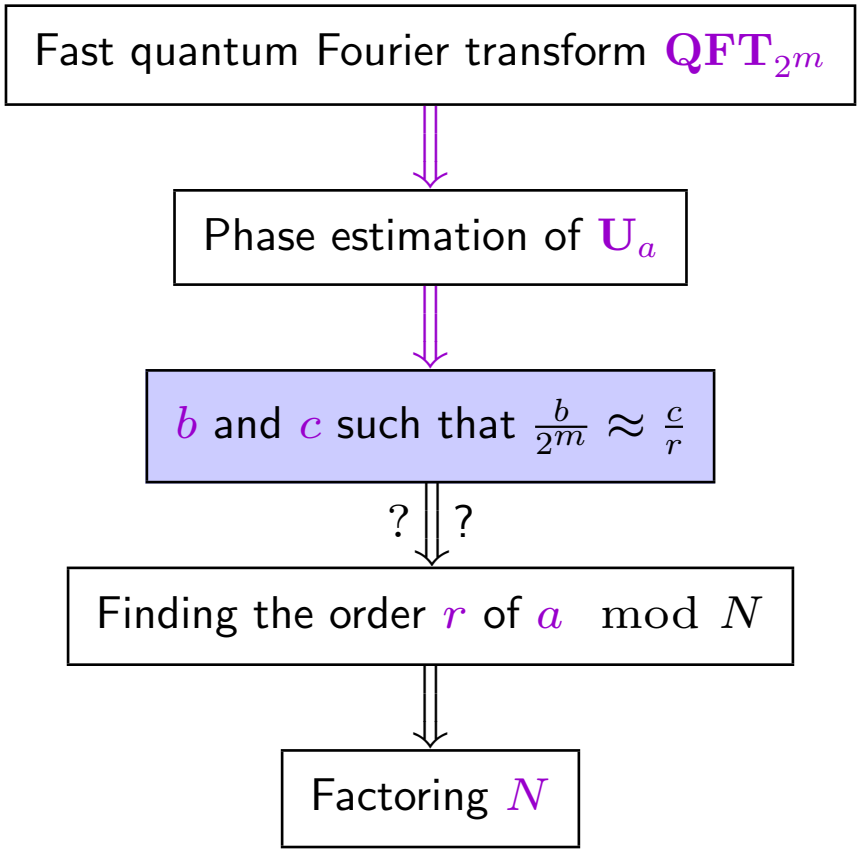

- This circuit produces the state

$$\frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} e^{\frac{2i\pi kx}{2^m}} |x\rangle |\phi\rangle = |\psi_k\rangle |\phi\rangle$$

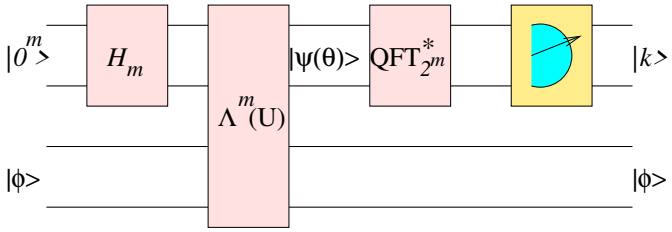
$$\begin{aligned} |\psi_k\rangle &= \mathbf{QFT}_{2^m} |k\rangle \\ |k\rangle &= \mathbf{QFT}^*_{2^m} |\psi_k\rangle \end{aligned}$$



# The global picture



# The general case




- Perform the same operations

$$|\psi(\theta)\rangle = \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} e^{2i\pi\theta x} |x\rangle$$

$$\mathbf{QFT}^*_{2^m} |x\rangle = \frac{1}{\sqrt{2^m}} \sum_{y=0}^{2^m-1} e^{-\frac{2i\pi xy}{2^m}} |y\rangle$$

$$\mathbf{QFT}^*_{2^m} |\psi(\theta)\rangle = \frac{1}{2^m} \sum_{x,y} e^{2i\pi\theta x} e^{-\frac{2i\pi xy}{2^m}} |y\rangle = \sum_{y=0}^{2^m-1} \alpha_y |y\rangle$$

$$\alpha_y \stackrel{\text{def}}{=} \frac{1}{2^m} \sum_{x=0}^{2^m-1} e^{2i\pi x(\theta - y/2^m)}$$

# The probability of measuring $|y\rangle$

$$
\begin{aligned}
p_y &\stackrel{\text{def}}{=} \text{prob. of measuring } |y\rangle \\
&= |\alpha_y|^2 \\
&= \frac{1}{2^{2m}} \left| \sum_{x=0}^{2^m-1} e^{2i\pi x(\theta - y/2^m)} \right|^2 \\
&= \frac{1}{2^{2m}} \left| \frac{e^{2i\pi(2^m\theta - y)} - 1}{e^{2i\pi(\theta - y/2^m)} - 1} \right|^2 \\
\max_y(p_y) &\geq \frac{4}{\pi^2} > 0.4
\end{aligned}
$$

## Exercise : lower bound on $\max_y(p_y)$

Let

$$\begin{aligned} y_0 &\stackrel{\text{def}}{=} \arg\min_y |\theta - \frac{y}{2^m}| \\ \varepsilon &\stackrel{\text{def}}{=} \theta - \frac{y_0}{2^m} \\ a &\stackrel{\text{def}}{=} \left| e^{2i\pi 2^m \varepsilon} - 1 \right| \\ b &\stackrel{\text{def}}{=} \left| e^{2i\pi\varepsilon} - 1 \right| \end{aligned}$$

1. Prove that $|\varepsilon| \leq \frac{1}{2^{m+1}}$
2. Prove that $a \geq 4|\varepsilon|2^m$
3. Prove that $b \leq 2\pi|\varepsilon|$
4. Prove the lower bound $\max_y(p_y) \geq \frac{4}{\pi^2}$

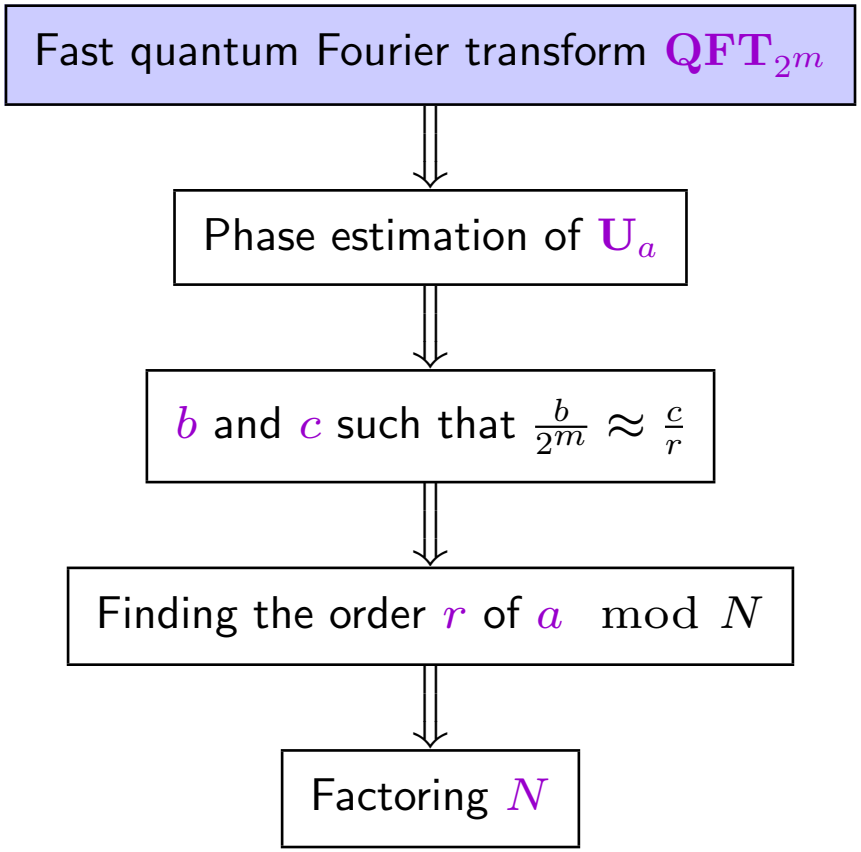
## The output of the phase estimation procedure

$$\theta = \frac{c}{r}$$

The previous algorithm outputs an integer $k$ with probability $\geq 0.4$ such that

$$\left| \frac{k}{2^m} - \frac{c}{r} \right| \leq \frac{1}{2^{m+1}}$$

# The global picture



## Efficient implementation of $\mathbf{QFT}_{2^m}$

$$\mathbf{R}_s \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & e^{2i\pi/2^s} \end{pmatrix}$$

$$\mathbf{R}_1 = \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \mathbf{R}_2 = \mathbf{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad \mathbf{R}_3 = \mathbf{T} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

- Efficient implementation with $\mathbf{H}$ and $\mathbf{T}$

$$\begin{aligned}
\mathbf{QFT}_{2^m} |k\rangle &= \frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} e^{2i\pi jk/2^m} |j\rangle \\
&= \frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} e^{2i\pi \left(\sum_{l=1}^{m} j_l 2^{m-l}\right) k/2^m} |j_1 \cdots j_m\rangle \\
&= \frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} \prod_{l=1}^{m} e^{2i\pi j_l k/2^l} |j_1 \cdots j_m\rangle \\
&= \bigotimes_{l=1}^{m} \frac{1}{\sqrt{2}} \left( |0\rangle + e^{2i\pi k/2^l} |1\rangle \right)
\end{aligned}$$

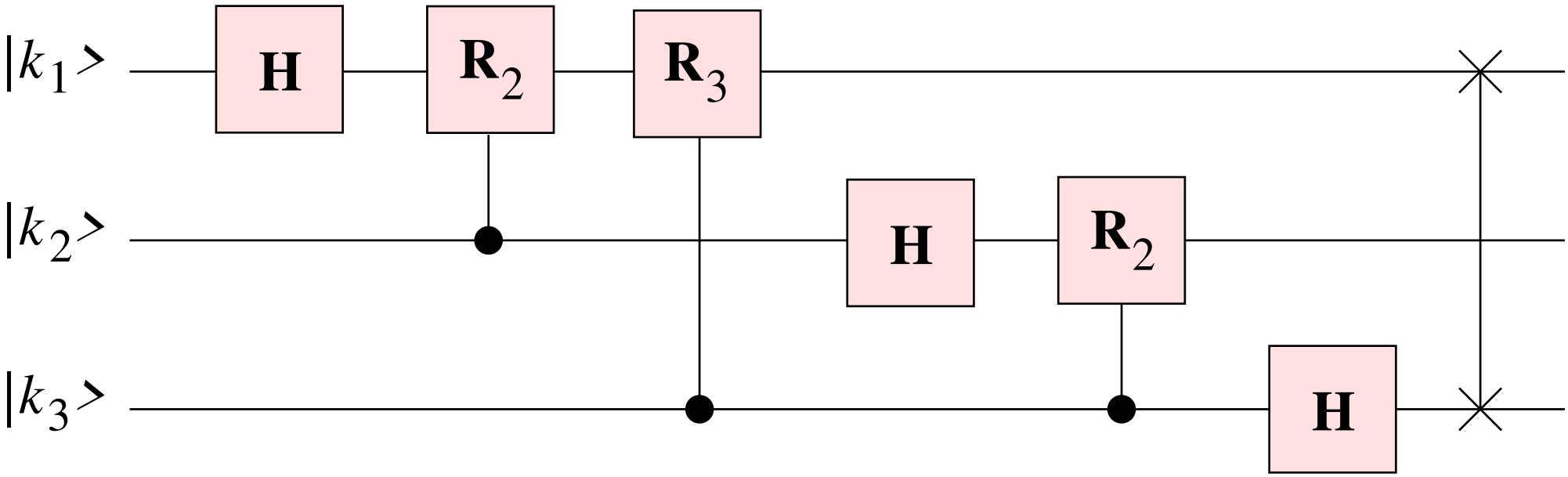
## Exercise

Give a quantum circuit implementing

1. $\mathbf{QFT}_2$
2. $\mathbf{QFT}_8$

## Solution

The first circuit is just the Hadamard transform. The second one is given by



## Quantum circuit complexity for $\mathbf{QFT}_{2^m}$

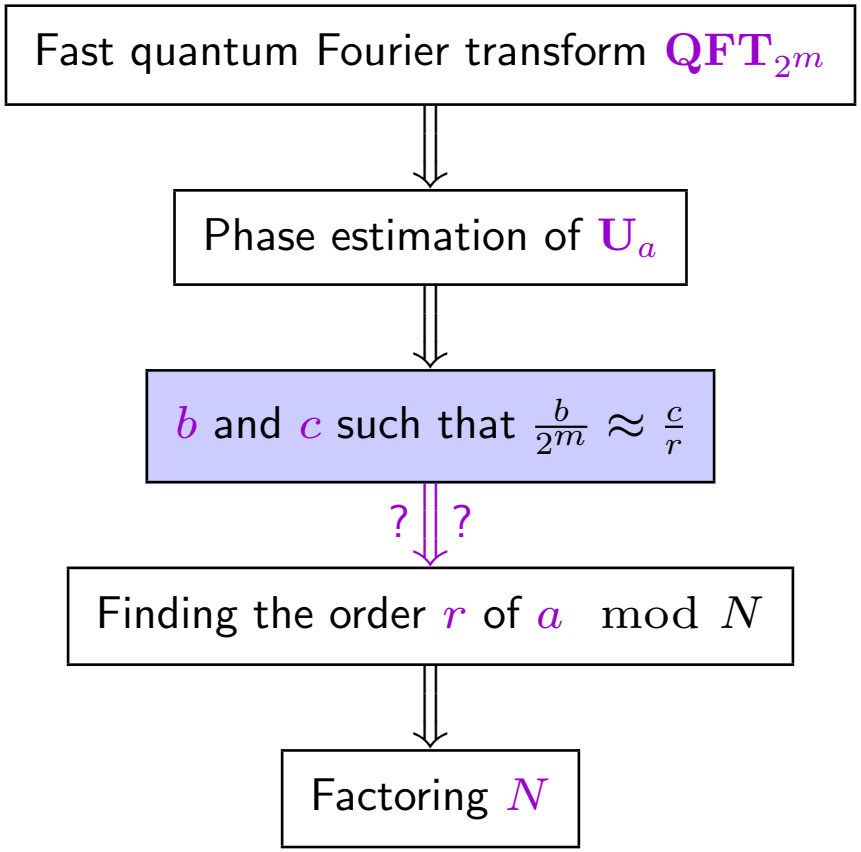
- Circuit of complexity $O(m^2)$ for $\mathbf{QFT}_{2^m}$
- Many of the $\mathbf{R}_s \approx \mathbf{Id}$ for $s \gg \log m \Rightarrow$ circuit of complexity $O(m \log m)$ for implementing $\mathbf{QFT}_{2^m}$ approximately

# Exercise : implementing $\mathrm{QFT}_{2^m}$ approximately

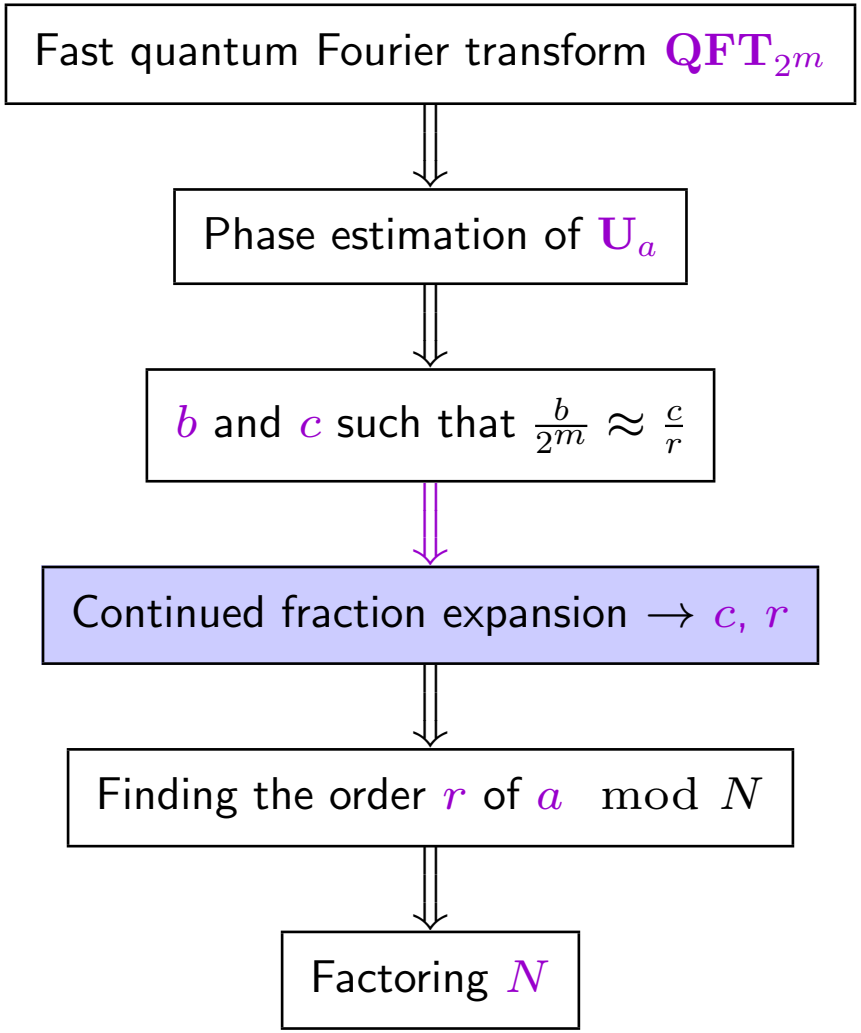
Operator norm of a matrix $\mathbf{M}$ defined by $\|\mathbf{M}\| \stackrel{\text{def}}{=} \sup_{\mathbf{x}:\|\mathbf{x}\|=1} \|\mathbf{M}\mathbf{x}\|$
Distance between two matrices $\mathbf{A}$ and $\mathbf{B}$ defined as $\|\mathbf{A}-\mathbf{B}\|$

1. compute $\|\mathbf{R}_s - \mathbf{Id}_2\|$
2. compute $\|\text{c-}\mathbf{R}_s - \mathbf{Id}_4\|$
3. compute $\|\text{c-}\mathbf{R}_s \otimes \mathbf{Id}_{2^{m-2}} - \mathbf{Id}_{2^m}\|$
4. if $\mathbf{U} = \mathbf{U}_1 \cdots \mathbf{U}_t$ and $\mathbf{U}' = \mathbf{U}_1 \cdots \mathbf{U}_{j-1}\mathbf{U}_{j+1} \cdots \mathbf{U}_t$ and the $\mathbf{U}_i$'s are unitary, show that $\|\mathbf{U} - \mathbf{U}'\| = \|\mathbf{Id} - \mathbf{U}_j\|$
5. Let $\mathbf{U}''$ be the unitary where we dropped $k$ $\mathbf{U}_i$'s in the product defining $\mathbf{U}$. Give an upper-bound on $\|\mathbf{U} - \mathbf{U}''\|$
6. Give a quantum circuit of gate complexity $O(m \log m)$ at distance $\leq 1/n$ from $\mathbf{QFT}_{2^m}$

# The global picture



# The global picture



## Information obtained from the phase estimation measurement

- Eigenvalue $\theta = \frac{c}{r}$ for some integer $c$
- Phase estimation measurement $\rightarrow b$ such that

$$\left| \frac{b}{2^m} - \frac{c}{r} \right| \leq \frac{1}{2^{m+1}}$$

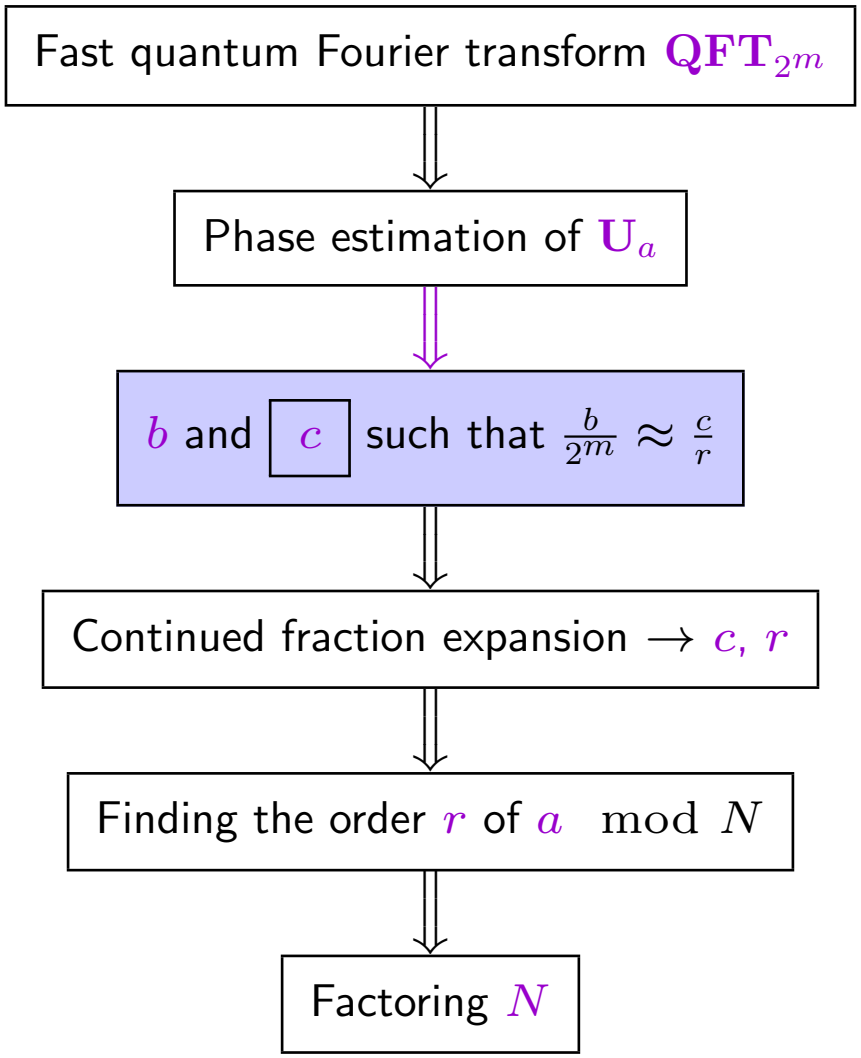
- Choose $m$ as

$$2^{m-1} \leq N^2 < 2^m$$

- Two distinct fractions each with denominator $\leq N$ must be at distance $\geq \frac{1}{N^2} > \frac{1}{2^m}$
- Therefore $c/r$ is the only fraction with denominator $\leq N$ at distance $\leq \frac{1}{2^{m+1}}$ from $b/2^m$
  $\Rightarrow$ obtained by continued fraction expansion

$$\frac{b}{q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots}}} \qquad \frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}}$$

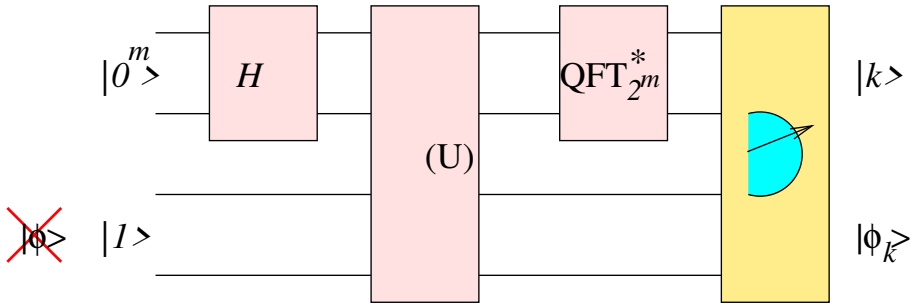
# The global picture



# Which $|\phi\rangle$ ?

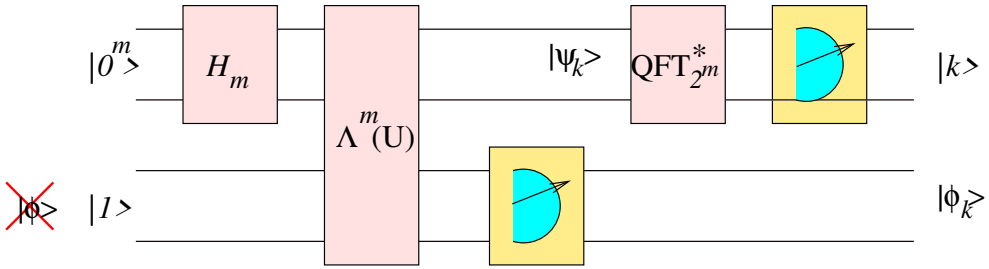
$$\begin{aligned} \mathbf{U}_a : |x\rangle &\mapsto |ax\rangle \\ \mathbf{U}_a |\phi_k\rangle &= e^{2i\pi k/r} |\phi_k\rangle \end{aligned}$$

- Which $|\phi_k\rangle$?
- Answer: none! Instead of an eigenvector $|\phi\rangle$ just $|1\rangle$!



# Why does this work?

$$\begin{aligned}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|\phi_k\rangle &= \frac{1}{r}\sum_{k=0}^{r-1}\sum_{l=0}^{r-1}e^{-2i\pi kl/r}\left|a^l\right\rangle \\ &= \left|a^0\right\rangle \\ &= |1\rangle\end{aligned}$$




- If we run the phase estimation on $|1\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|\phi_k\rangle$ then

$$\begin{aligned}\text{just before measurement} \quad &: \quad \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|\psi_k\rangle\,|\phi_k\rangle \\ \text{after first measurement} \quad &\rightarrow \quad |\psi_k\rangle\,|\phi_k\rangle \text{ with prob. } 1/r\end{aligned}$$