Quantum Algorithms (5)

Hung-Wei Tseng

Shor’s Algorithm

Shor's algorithm

- Reducing the integer factorization problem into the period finding problem
  - $f(x) = a^x \bmod N = 1$ if a and N are positive integers, a is less than N, and they have no common factors.
  - Find the period, or order (r), the smallest (non-zero) integer makes f(x) = 1
  - Shor's solution was to use quantum phase estimation on the unitary operator to find r:
    $U|y\rangle \equiv |ay \bmod N\rangle$
  - The factors of N are $gcd(a^{\frac{r}{2}} \pm 1, N)$ and we are done.

Why $a^{\frac{r}{2}}$

- Since r is the period of $f(x) = a^x \bmod N$, $f(x) = a^r \bmod N = 1$
- If r is even

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

$$a^r - 1 \bmod N = 0$$

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

- Let $a_0 = a^{\frac{r}{2}} - 1$ and $a_1 = a^{\frac{r}{2}} + 1$, this implies $N \,|\, (a^{\frac{r}{2}} - 1)a^{\frac{r}{2}} + 1$ or $N \,|\, a_0 a_1$
- Since r is the smallest integer such that $a^r \bmod N = 1$, N cannot divide a_0 — N has a non-trivial factor in common with either a_0 or a_1

How QPE can help find the period?

- For example, a = 3 and N = 35:

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

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

$$U: |u_0\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |a^k \bmod N\rangle$$
$$|u_0\rangle = \frac{1}{\sqrt{12}}(|1\rangle + |3\rangle + |9\rangle \ldots + |4\rangle + |12\rangle)$$
$$U|u_0\rangle = \frac{1}{\sqrt{12}}(U|1\rangle + U|3\rangle + U|9\rangle \ldots + U|4\rangle + U|12\rangle)$$
$$= \frac{1}{\sqrt{12}}(|3\rangle + |9\rangle + |27\rangle \ldots + |12\rangle + |1\rangle)$$
$$= |u_0\rangle$$

How QPE can help find the period? (2)

- Let’s look at the case in which the phase of the kth state is proportional to k:

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

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

For a=3, N=35,

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

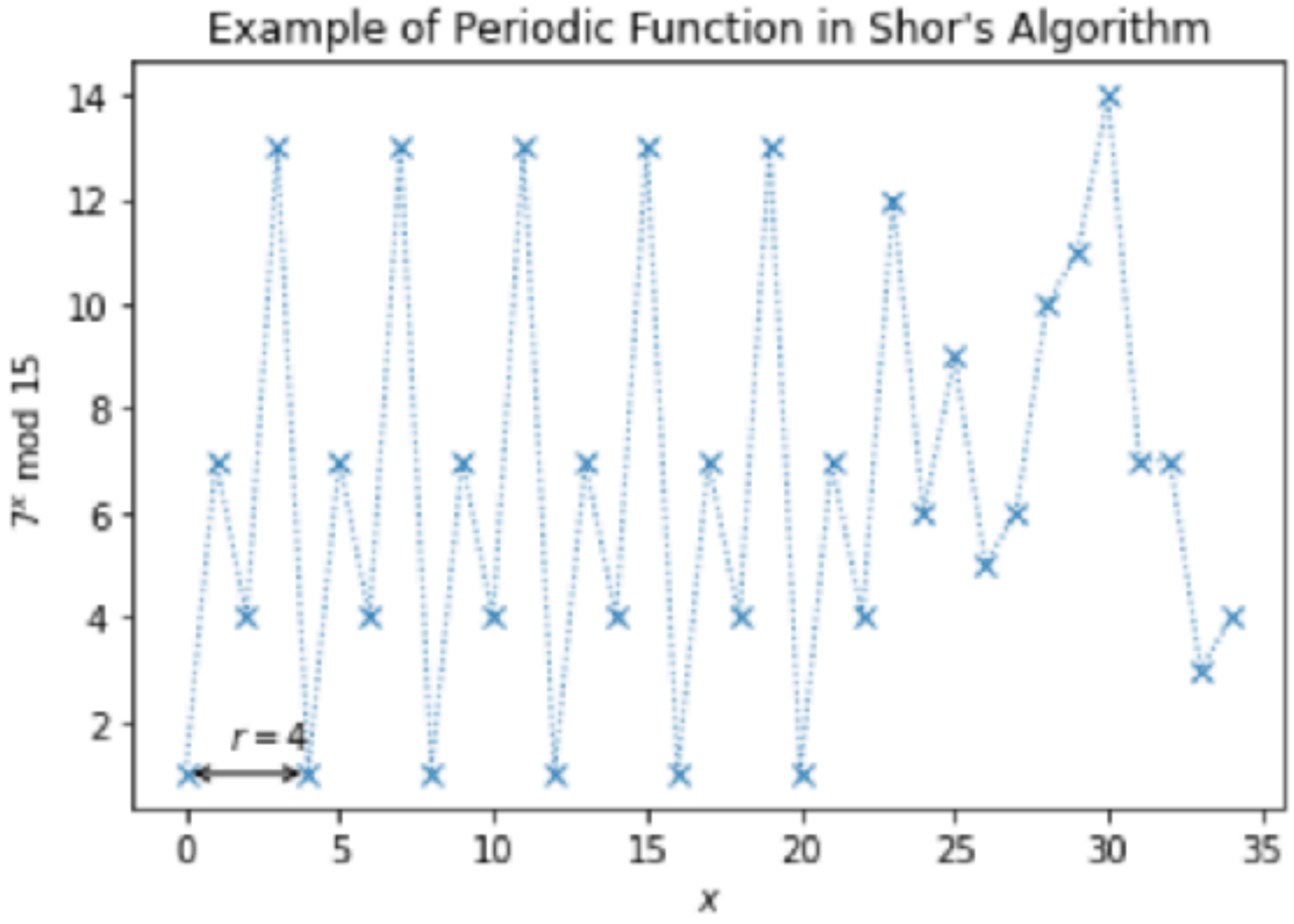
$$U|u_1\rangle = \frac{1}{\sqrt{12}}(|3\rangle + e^{-\frac{2\pi i}{12}}|9\rangle + e^{-\frac{4\pi i}{12}}|27\rangle \ldots + e^{-\frac{20\pi i}{12}}|12\rangle + e^{-\frac{22\pi i}{12}}|1\rangle)$$

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

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

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

$3^6 = 729$, gcd(728, 35) = 7, gcd(730, 35)=5



Find the period *r* of this function

$$\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|x^j \bmod N\rangle$$

Approximate as finding *r* in phase estimation

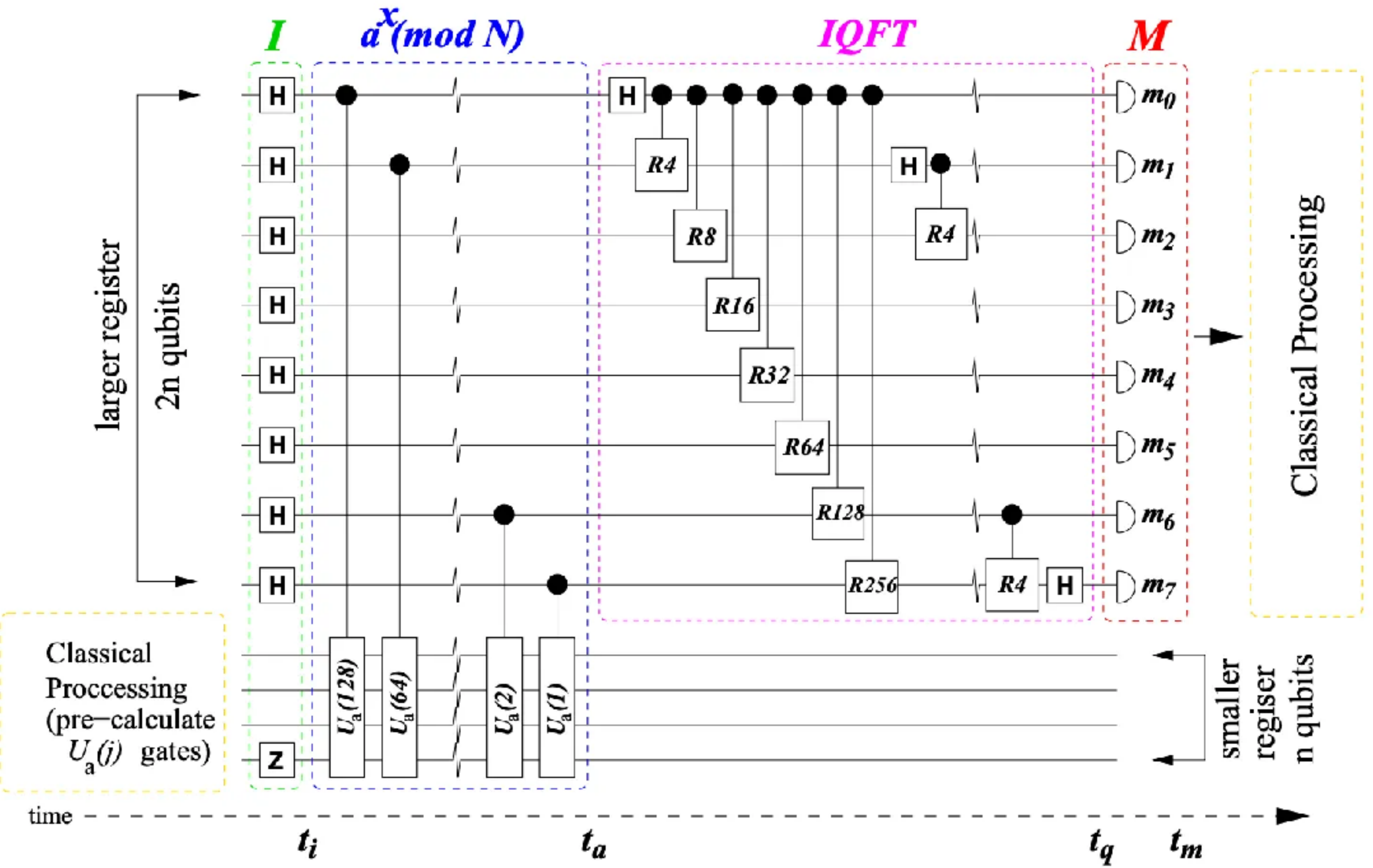
$$\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|x^j \bmod N\rangle \rightarrow \frac{1}{\sqrt{r2^t}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^t-1}e^{2\pi i s j/\underline{r}}|j\rangle|u_s\rangle$$

eigenvector for U where $U|y\rangle = |xy \mod N\rangle$

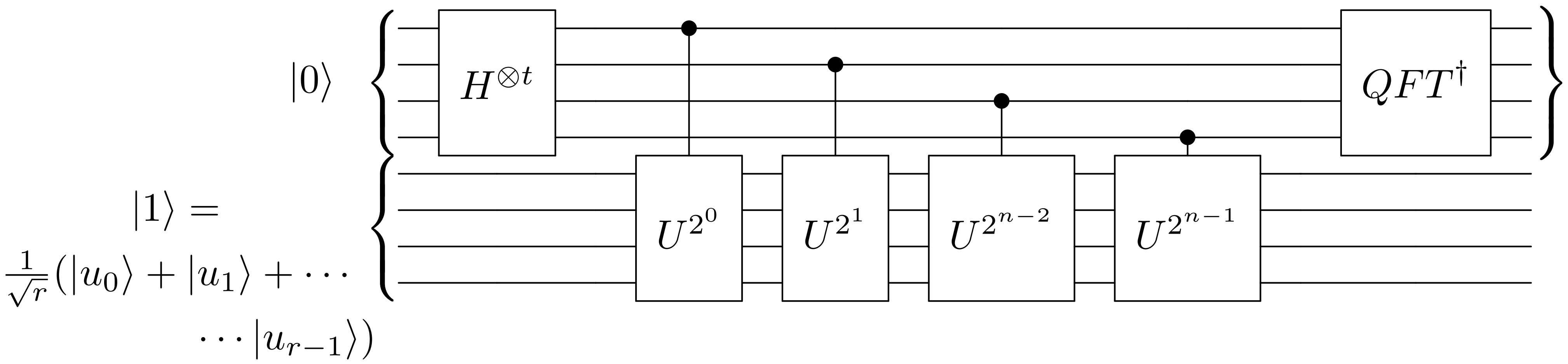
x = 0, 1, 2 , ...

$$\frac{1}{\sqrt{2^q}}\left[|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + |5\rangle|7\rangle + |6\rangle|4\rangle + \cdots\right]$$

f(x) = 7^x mod 15   *f(0) =1 , f(1) = 7, f(2) = 49 mode 15 = 4*


I
a^x(mod N)
IQFT
M
larger register
2n qubits
H
H
H
H
H
H
H
H
Z
U_a(128)
U_a(64)
U_a(2)
U_a(1)
H
R4
R8
R16
R32
R64
R128
R256
H
R4
R4
H
m0
m1
m2
m3
m4
m5
m6
m7
Classical Processing
Classical
Proccessing
(pre−calculate
U_a(j) gates)
smaller
regiser
n qubits
time
t_i
t_a
t_q
t_m

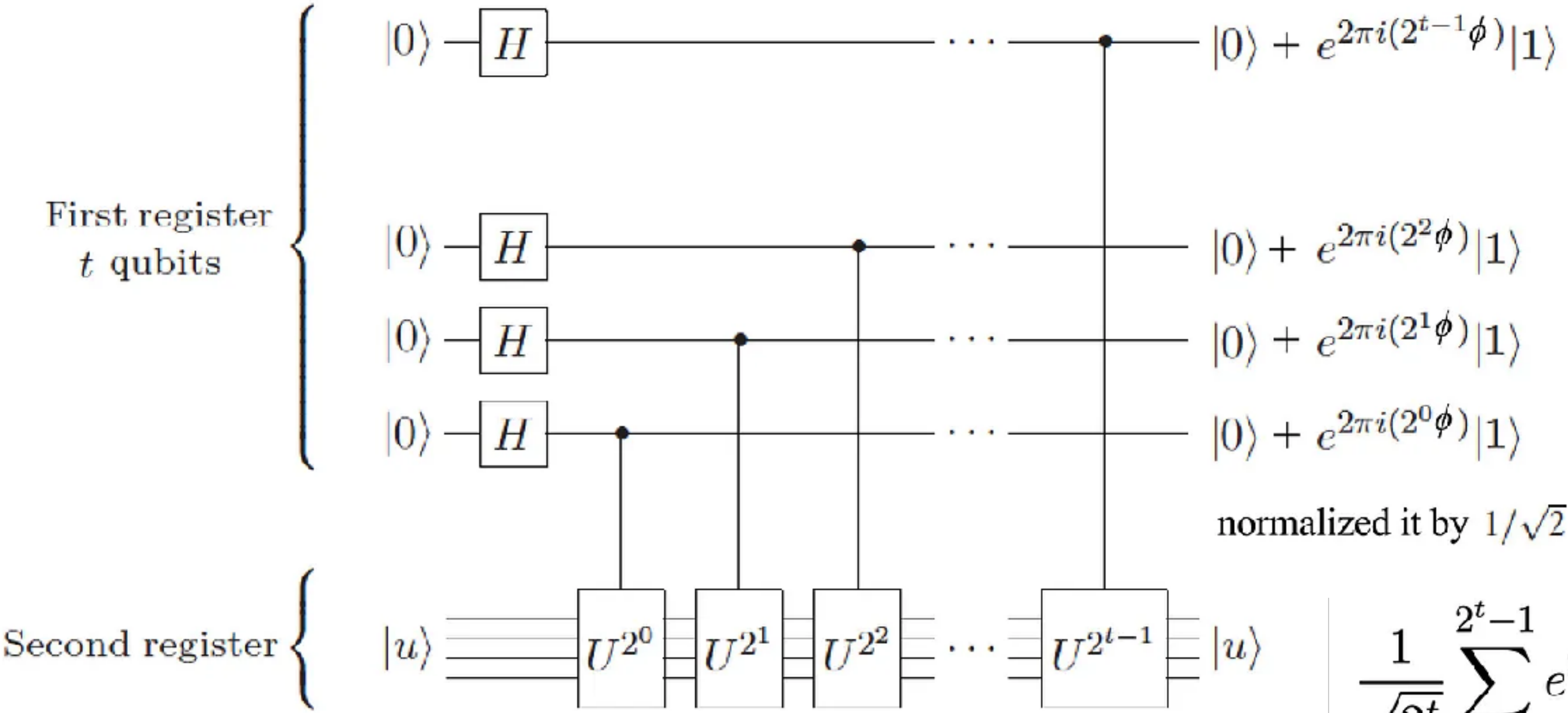
The Unitary using continued fraction


$|0\rangle$
$|1\rangle = \frac{1}{\sqrt{r}}(|u_0\rangle + |u_1\rangle + \cdots \cdots |u_{r-1}\rangle)$
$H^{\otimes t}$
U^{2^0}
U^{2^1}
$U^{2^{n-2}}$
$U^{2^{n-1}}$
$QFT^\dagger$

$$\frac{1}{\sqrt{r}}(|2^n \cdot \tfrac{1}{r}\rangle + |2^n \cdot \tfrac{2}{r}\rangle + \cdots \cdots |2^n \cdot \tfrac{r-1}{r}\rangle)$$

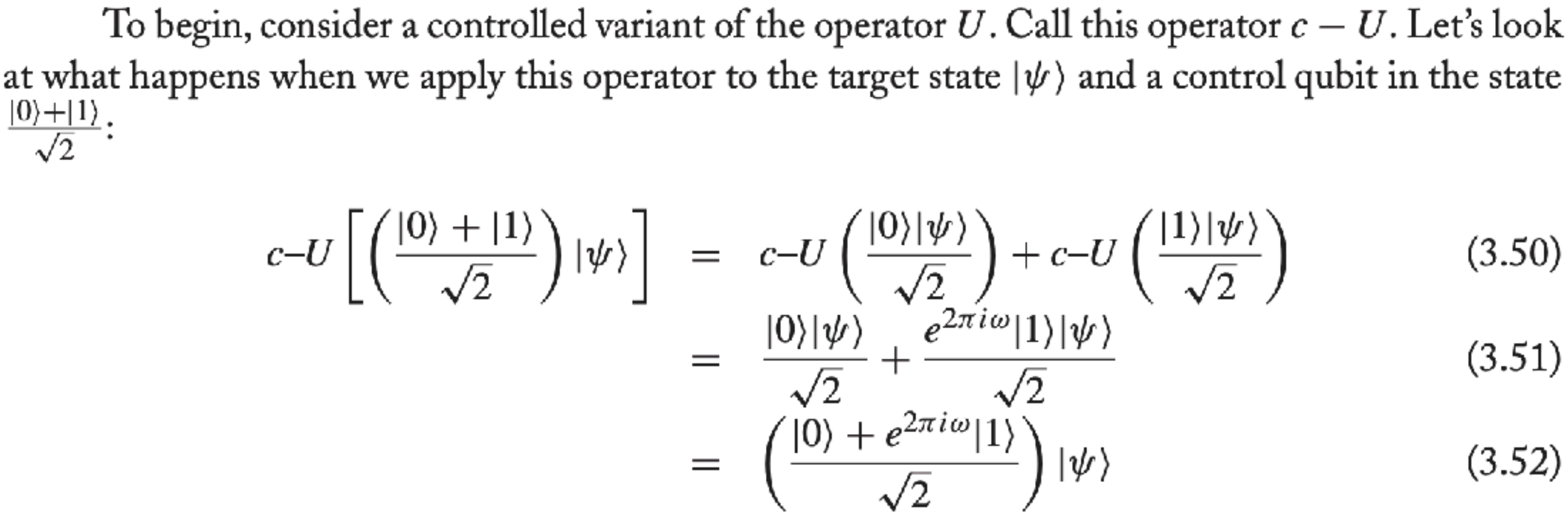
$$x = b_0 + \operatorname*{K}_{i=1}^{\infty} \frac{a_i}{b_i}$$

To reduce the number of measurements, the U is redesigned to


First register
t qubits
Second register
$|0\rangle$
H
$|u\rangle$
U^{2^0}
U^{2^1}
U^{2^2}
$U^{2^{t-1}}$
$|0\rangle + e^{2\pi i(2^{t-1}\phi)}|1\rangle$
$|0\rangle + e^{2\pi i(2^2\phi)}|1\rangle$
$|0\rangle + e^{2\pi i(2^1\phi)}|1\rangle$
$|0\rangle + e^{2\pi i(2^0\phi)}|1\rangle$
$|u\rangle$

normalized it by $1/\sqrt{2}$

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



To begin, consider a controlled variant of the operator U. Call this operator $c-U$. Let's look at what happens when we apply this operator to the target state $|\psi\rangle$ and a control qubit in the state $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$:

$$\begin{aligned} c\text{–}U\left[\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|\psi\rangle\right] &= c\text{–}U\left(\frac{|0\rangle|\psi\rangle}{\sqrt{2}}\right)+c\text{–}U\left(\frac{|1\rangle|\psi\rangle}{\sqrt{2}}\right) && (3.50)\\ &= \frac{|0\rangle|\psi\rangle}{\sqrt{2}}+\frac{e^{2\pi i\omega}|1\rangle|\psi\rangle}{\sqrt{2}} && (3.51)\\ &= \left(\frac{|0\rangle+e^{2\pi i\omega}|1\rangle}{\sqrt{2}}\right)|\psi\rangle && (3.52) \end{aligned}$$

As we can see above, we have introduced the eigenvalue $e^{2\pi i\omega}$ into the state of the control register. If we had chosen an operator U^{2^j} instead of U, the state of the control register would have become

$$\frac{|0\rangle + e^{2\pi i(2^j\omega)}|1\rangle}{\sqrt{2}} \tag{3.53}$$

since U^{2^j} has an eigenvalue $(e^{2\pi i\omega})^{2^j} = e^{2\pi i(2^j\omega)}$. The state of this control register should look eerily similar to the states of the individual qubits at the beginning of the phase estimation algorithm. In fact, if we set $j = n - m$, the resulting state after the controlled operations is precisely the state of the m-th qubit at the start of the phase estimation algorithm. If we prepare n control registers in the state $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and apply U^{n-m} to the m-th qubit, we will have prepared an n-qubit state that we can supply as input to the phase estimation algorithm to get an estimate of the parameter ω. Figure 3.3 shows a circuit for doing this. Note that we can prepare the n control registers into the state

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n} \tag{3.54}$$

by applying the QFT to the state $|0\rangle^{\otimes n}$.

How can we arrive at this mapping from the sequence of controlled operations we just saw? We can do this by analyzing what happens when we apply the controlled sequence of operations to the state vector $|y\rangle|z\rangle$ (as described in [149]):

$$\begin{aligned}
|z\rangle|y\rangle &\xrightarrow{\textit{Controlled operations}} |z\rangle U^{z_n 2^{n-1}} \dots U^{z_1 2^0}|y\rangle && (3.56)\\
&= |z\rangle U^{z_n 2^{n-1}} \dots U^{z_2 2}|y a^{z_1 2^0} \mod N\rangle && (3.57)\\
&= |z\rangle U^{z_n 2^{n-1}} \dots U^{z_3 2^2}|y a^{z_2 2^1} a^{z_1 2^0} \mod N\rangle. && (3.58)
\end{aligned}$$

Continuing in this way for all the controlled operations, we get

$$\begin{aligned}
|z\rangle|y\rangle &\xrightarrow{\textit{Controlled operations}} |z\rangle|y a^{z_n 2^{n-1}} \dots a^{z_1 2^0} \mod N\rangle && (3.59)\\
&= |z\rangle|y a^{z} \mod N\rangle. && (3.60)
\end{aligned}$$

Grover’s Algorithm

The search problem

- Suppose you are given a large list of N items. Among these items there is one item with a unique property that we wish to locate; we will call this one the winner w. Think of each item in the list as a box of a particular color. Say all items in the list are gray except the winner w, which is purple.

Classical solution

- Check on average $\frac{N}{2}$ of these boxes

  — the worst case, all N of them

  — $O(N)$

Grover's algorithm

- Setup: superposition N-qubits

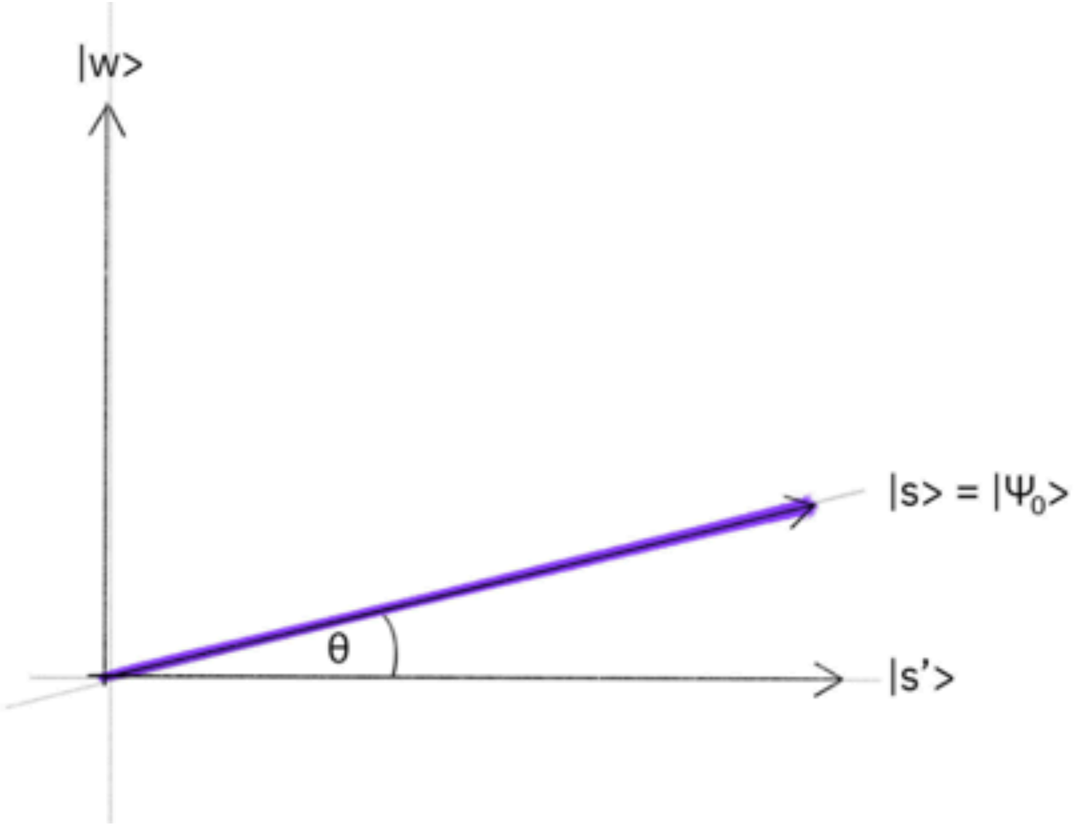
  $$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

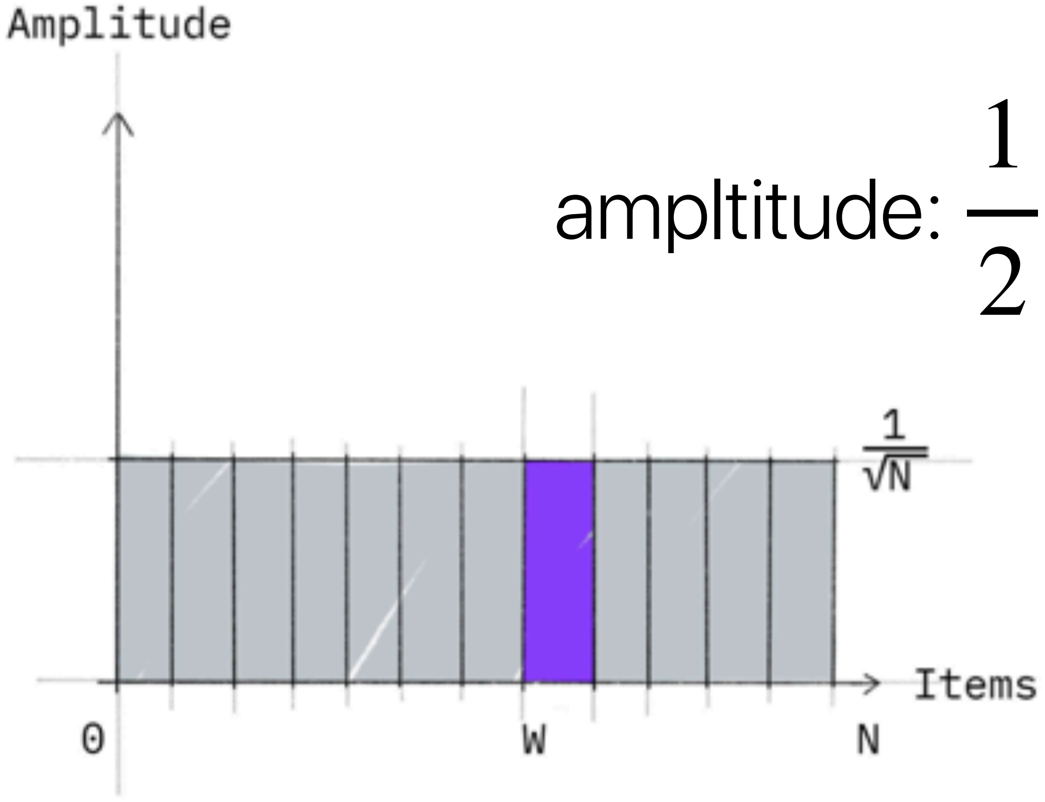
  $|s\rangle = \sin\theta|w\rangle + \cos\theta|s'\rangle,$ where $\theta = \arcsin\langle s|w\rangle = \arcsin\frac{1}{\sqrt{N}}$

  — any $|x\rangle$ would have a equal probability to be measured, so the probability of each state is now $\frac{1}{N} = \frac{1}{2^n}$

- The main algorithm: amplitude amplification — amplifies the amplitude of the marked item, but shrinks the other items' amplitude
  - Apply the oracle reflection U_f to the state $|s\rangle$ that changes amplitude of the $|w\rangle$ state to negative, which in turn means that the average amplitude has been lowered
  - Apply an additional reflection (U_s) about the state $|s\rangle$:$U_s = 2|s\rangle\langle s| - 1$. This transformation maps the state to $U_sU_f|s\rangle$ and completes the transformation.

Initialization

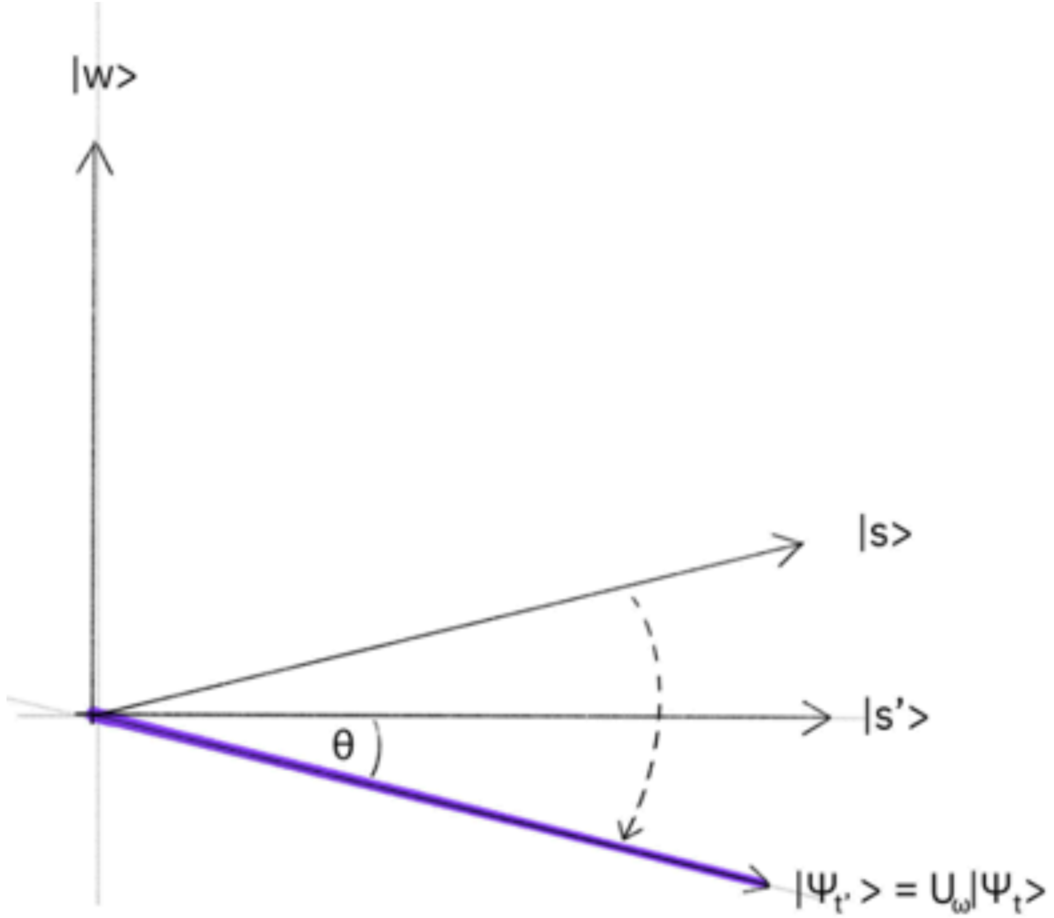


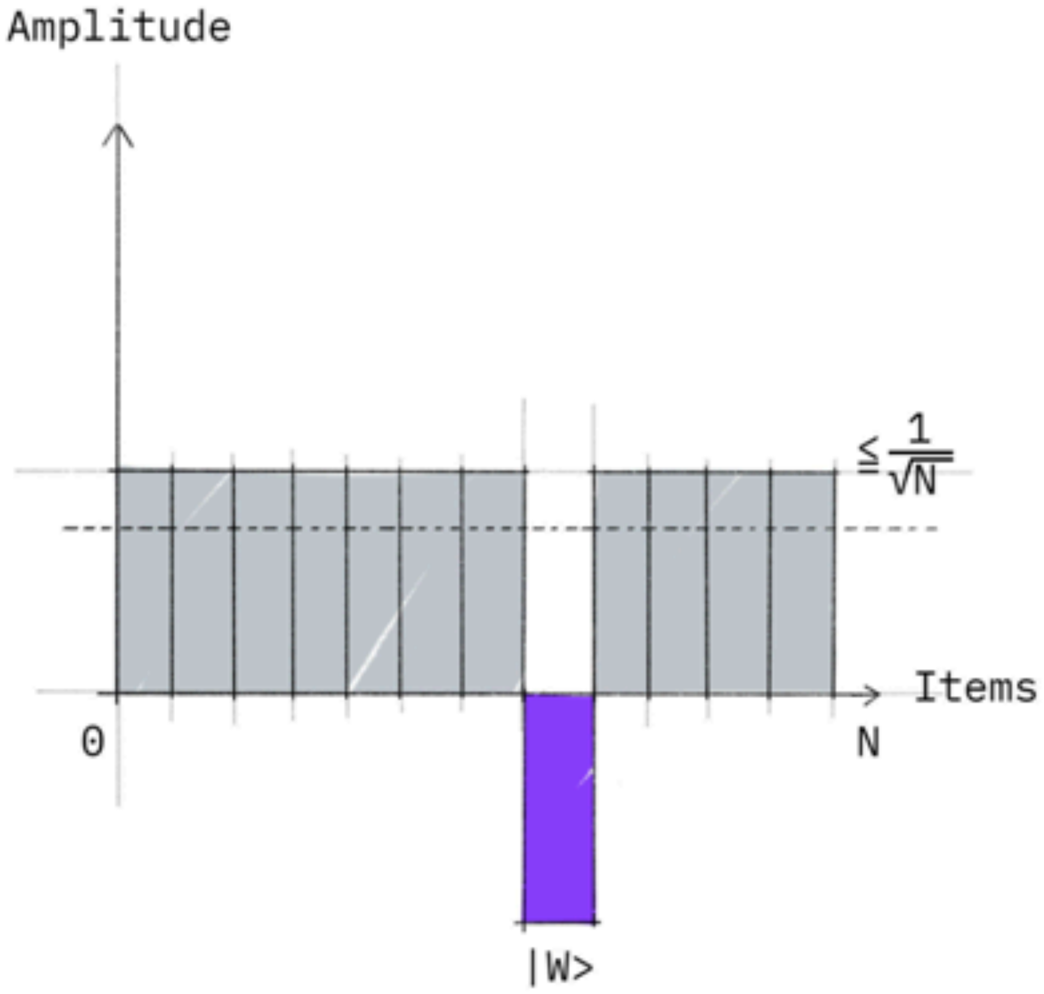


amplititude: $\dfrac{1}{2}$

- any $|x\rangle$ would have a equal probability to be measured, so the probability of each state is now $\dfrac{1}{N} = \dfrac{1}{2^n}$

Change the phase of the winner

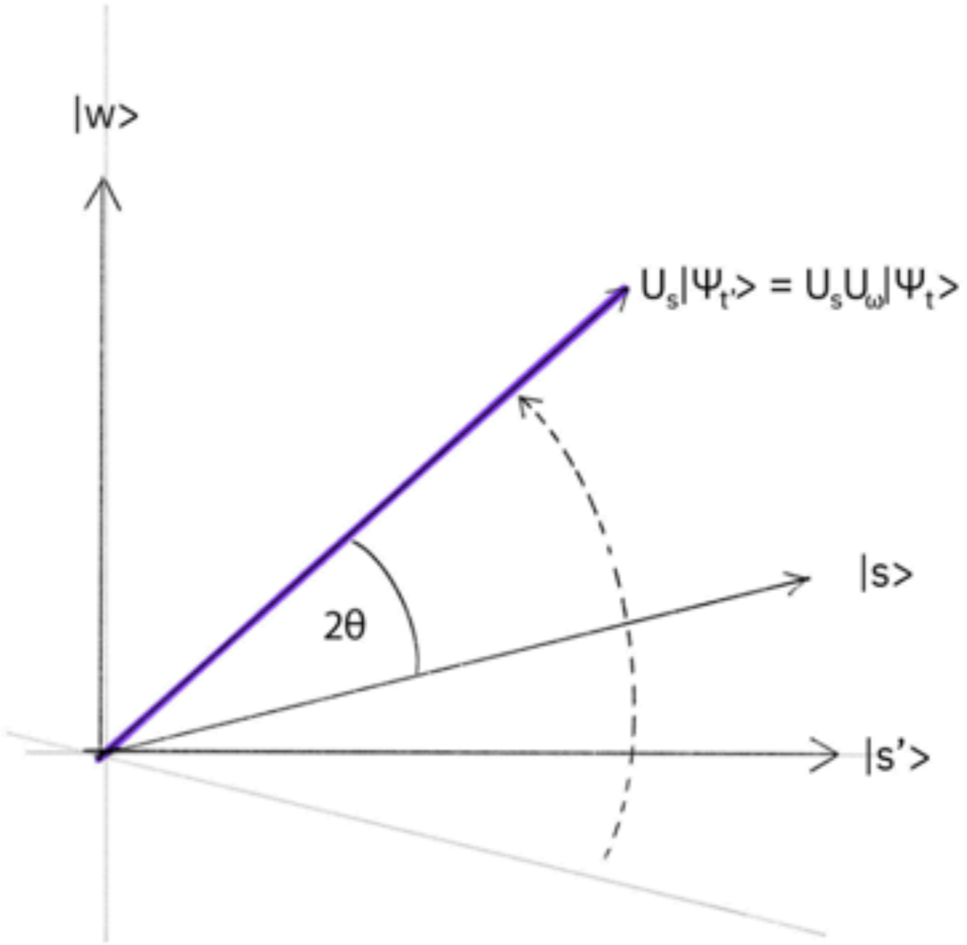


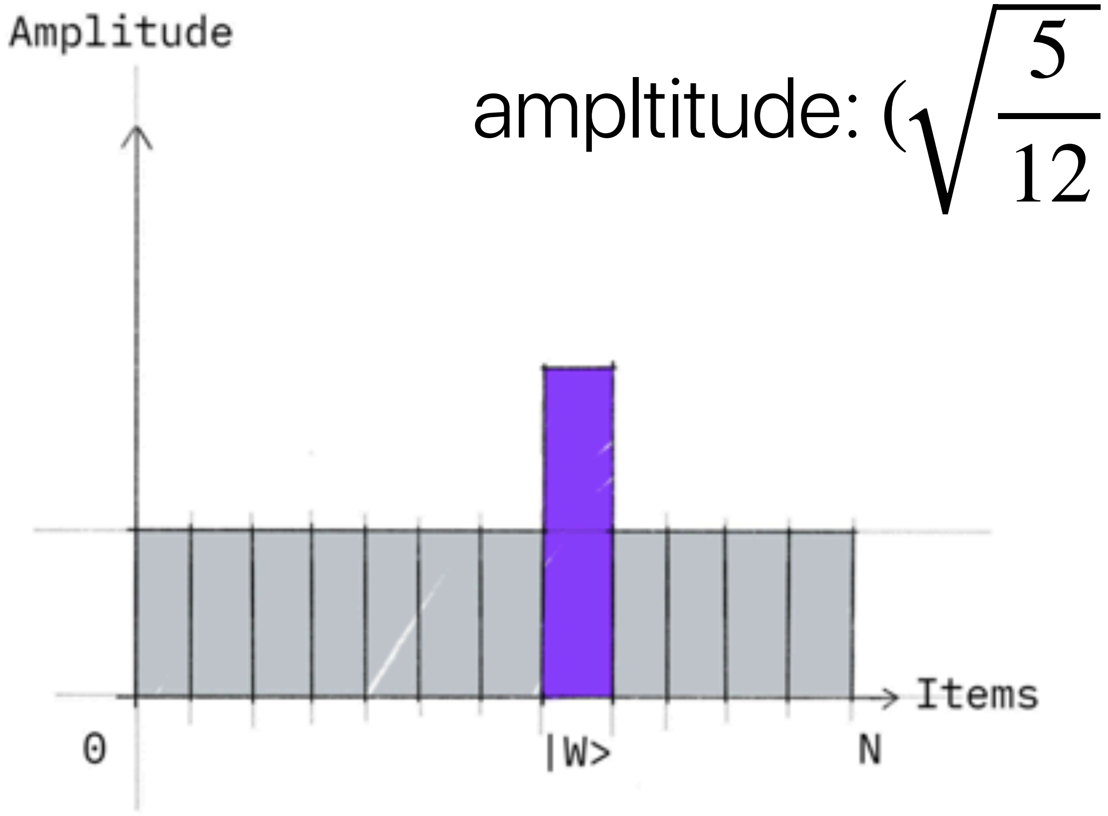


We apply the oracle reflection Uf to the state $|s\rangle$.

ampltitude: $(\sqrt{\frac{5}{12}}, -\frac{1}{2})$

Additional reflection





ampltitude: $(\sqrt{\frac{5}{12}}, -\frac{1}{2})$

We now apply an additional reflection (Us) about the state $|s\rangle$: $Us=2|s\rangle\langle s|-\mathbb{1}$

Creating the "oracle"

$$U_\omega |x\rangle = \begin{cases} |x\rangle & \text{if } x \neq \omega \\ -|x\rangle & \text{if } x = \omega \end{cases}$$

$$U_\omega |x\rangle = (-1)^{f(x)} |x\rangle$$

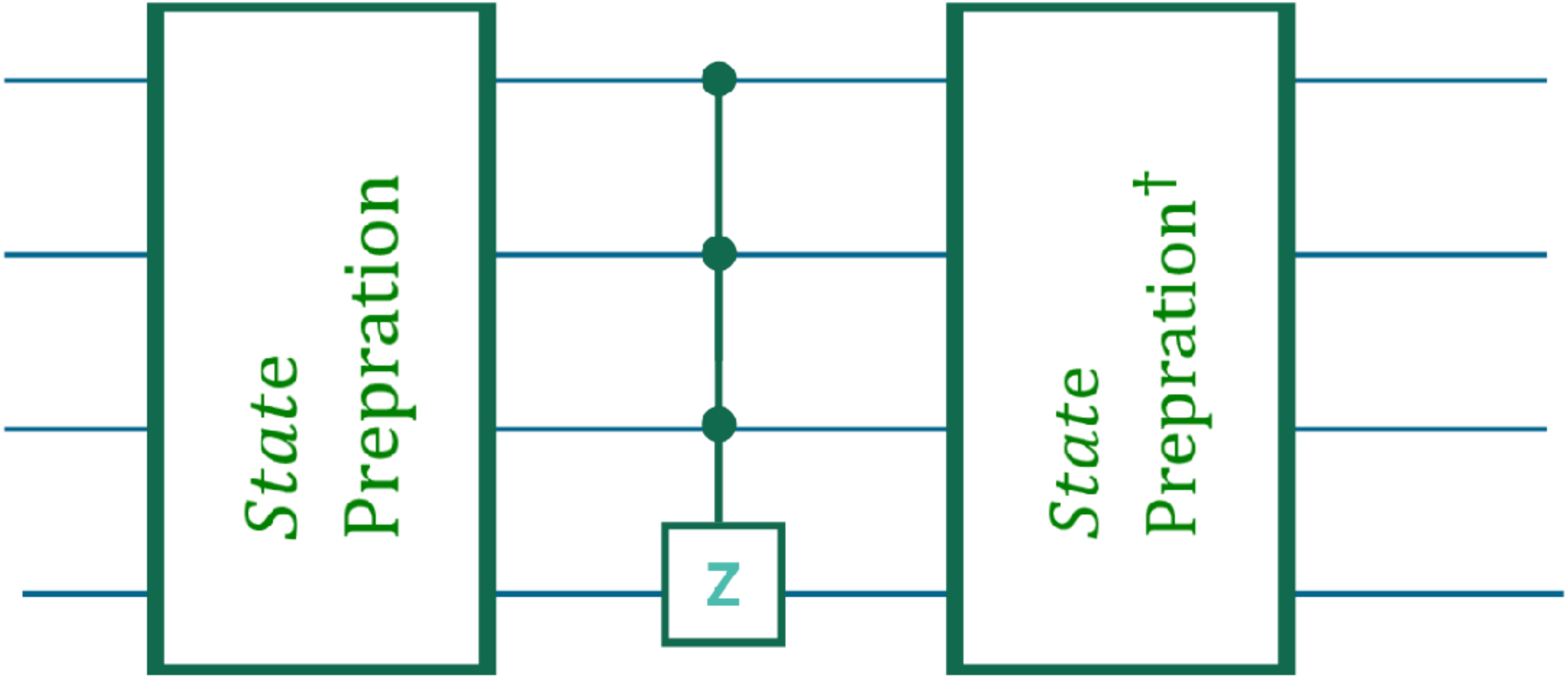
$$U_\omega = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{array}{l} \\ \\ \\ \\ \\ \leftarrow \omega = 101 \\ \\ \\ \end{array}$$

$$U_\omega = \begin{bmatrix} (-1)^{f(0)} & 0 & \cdots & 0 \\ 0 & (-1)^{f(1)} & \cdots & 0 \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & (-1)^{f(2^n-1)} \end{bmatrix}$$

Diffusion

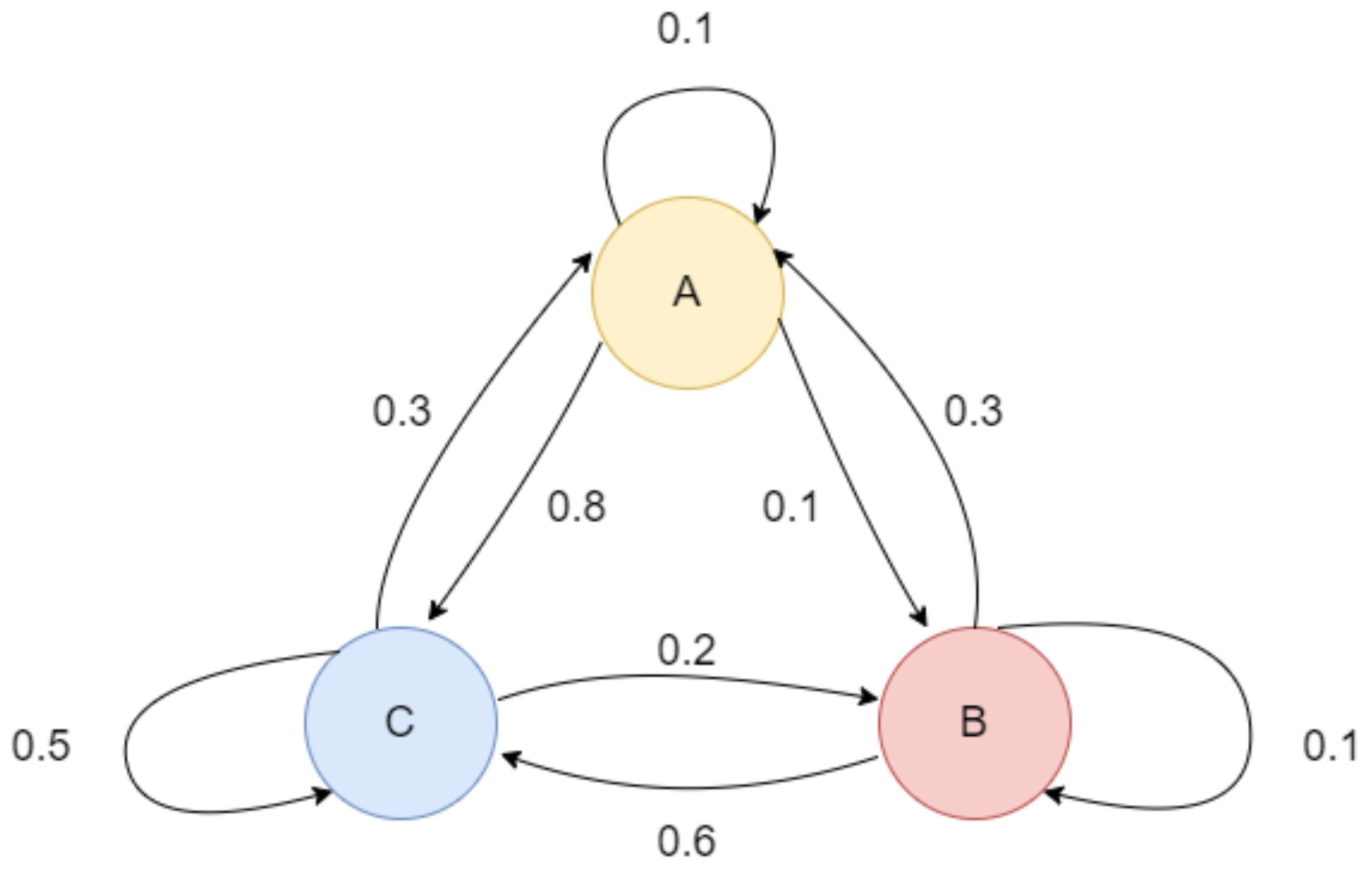
- Add additional $U_s = 2|s\rangle\langle s| - 1$ and negative phase orthogonal to $|s\rangle$
- Make $|s\rangle \rightarrow |0\rangle$ by $H^{\otimes n}|s\rangle = |0\rangle$
- Make $|0\rangle \rightarrow |s\rangle$ by $H^{\otimes n}U_0H^{\otimes n} = U_s$

Diffusion operation



Quantum Walk Search

Markov Chain



$$P = \begin{pmatrix} 0.1 & 0.3 & 0.3 \\ 0.1 & 0.1 & 0.2 \\ 0.8 & 0.6 & 0.5 \end{pmatrix}$$

Quantum Walks

- The quantum equivalent of the classical Markov chain
  - Due to superposition, a quantum walk will take all possible paths simultaneously until we measure the circuit
  - Due to quantum interference, some state will cancel out
  - Faster than classical ones, since we can cancel out wrong answers quickly

Coined quantum walks

- A coined quantum is a walk on the nodes (states) in a graph — Two-sides in coin-flipping — computational basis is $\{|0\rangle, |1\rangle\}$
- The walker can move between states that are connected with an edge
- In the coin model, we have
  - Two quantum states $\mathscr{H} = \mathscr{H}_C \otimes \mathscr{H}_P$
    - Positions $\mathscr{H}_P$
    - Coin orientation $\mathscr{H}_C$
  - Two operators
    - The coin operator C

      Hadamard coin: $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ and Grover coin: $G = \begin{bmatrix} \frac{2}{n} - 1 & \frac{2}{n} & \dots & \frac{2}{n} \\ \frac{2}{n} & \frac{2}{n} - 1 & \dots & \frac{2}{n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{n} & \frac{2}{n} & \dots & \frac{2}{n} - 1 \end{bmatrix}$

    - The shift operator S

      $S|0\rangle|j\rangle = |0\rangle|j+1\rangle$

      $S|1\rangle|j\rangle = |1\rangle|j-1\rangle$
  - $U = SC, |\psi(t)\rangle = U^t|\psi(0)\rangle$