CLASSICAL AND QUANTUM COMPUTATION

QUANTUM ALGORITHMS

Quantum Fourier transform

Quantum Fourier transform is an efficient way of performing a Fourier transform of quantum mechanical amplitudes.

It does not speed up classical task of performing a Fourier transform of classical data but it enables *phase estimation*, the approximation of the eigenvalues of a unitary operator under certain circumstances.

Phase estimation allows to solve other interesting problems including quantum computation of *molecular electronic structure* and *factorization*.

Discrete Fourier transform

Input:

a vector of N complex numbers $x_0, x_1, \ldots, x_{N-1}$;

Output:

a vector of N complex numbers $y_0, y_1, \ldots, y_{N-1}$ defined by

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \, e^{2\pi i jk/N}$$

$$\frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{pmatrix} \qquad \omega = e^{2\pi i/8}$$

Quantum Fourier transform

Quantum Fourier transform on an orthonormal basis $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ is defined to be a linear operator

$$|j\rangle \quad \rightarrow \quad \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} \, |k\rangle$$

Equivalently, the quantum Fourier transform on an arbitrary quantum state is given as

$$\sum_{j=0}^{N-1} x_j \, |j\rangle \quad \rightarrow \quad \sum_{k=0}^{N-1} y_k \, |k\rangle$$

where the amplitudes y_k are the discrete Fourier transform of the amplitudes x_j.

Quantum Fourier transform circuit

We consider $N = 2^n$, $n \in \mathbb{Z}$ and the computational basis $|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle$.

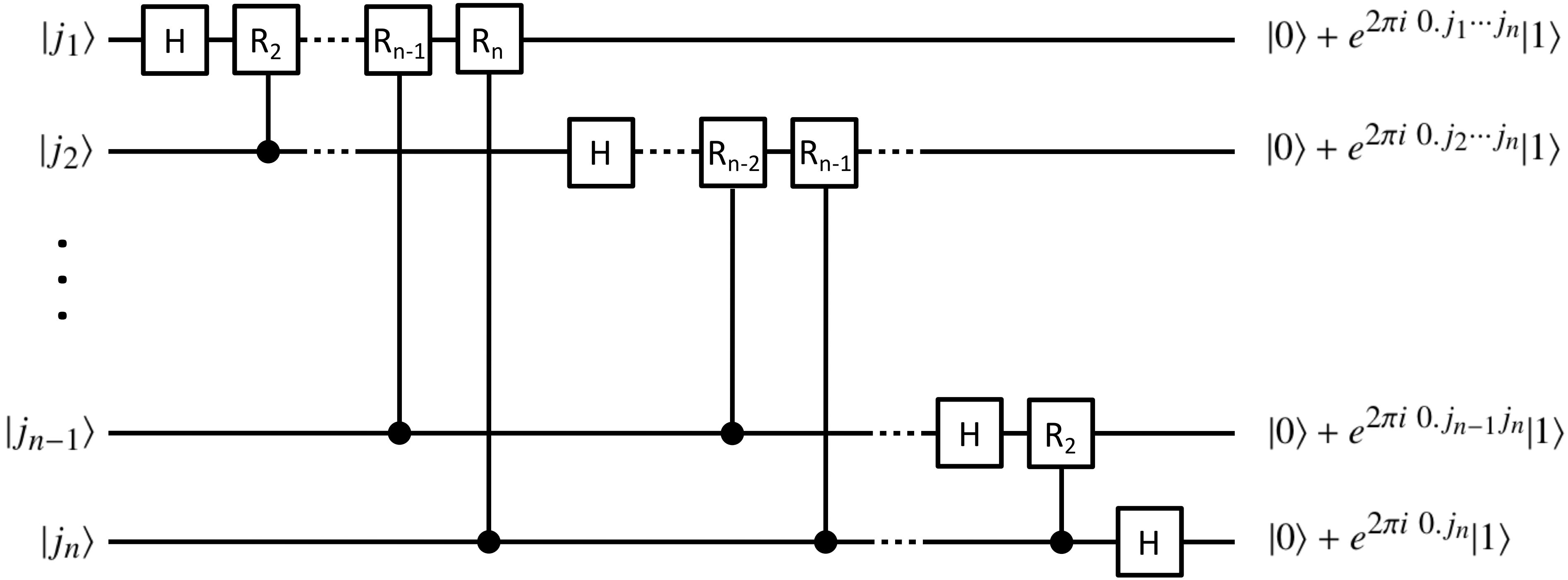
We write the state $|j\rangle$ in binary representation $j = j_1 j_2 \ldots j_n$, or more formally $j = j_1 2^{n-1} + j_2 2^{n-2} + \ldots + j_n 2^0$.

Also, we adopt the notation $0.j_l j_{l+1} \ldots j_m$ to represent the *binary fraction* $j_l/2 + j_{l+1}/4 + \ldots + j_m/2^{m-l+1}$.

The new notation allows us to represent quantum Fourier transform in a *product* form that is well suited for construction of an efficient quantum circuit computing the transform. It will also provide insights into the algorithms based upon QFT.

The quantum Fourier transform can be rewritten as follows

$$
\begin{aligned}
|j\rangle \quad &\rightarrow \quad \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i jk/2^n} \, |k\rangle \\
&= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} e^{2\pi i j \left(\sum_{l=1}^{n} \; k_l \, 2^{-l}\right)} |k_1 \dots k_n\rangle \\
&= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l \, 2^{-l}} \, |k_l\rangle \\
&= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} e^{2\pi i j k_l \, 2^{-l}} \, |k_l\rangle \right] = \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i j \, 2^{-l}} |1\rangle \right] \\
&= \frac{\left(|0\rangle + e^{2\pi i \; 0.j_n} \, |1\rangle\right)\left(|0\rangle + e^{2\pi i \; 0.j_{n-1} j_n} \, |1\rangle\right) \dots \left(|0\rangle + e^{2\pi i \; 0.j_1 j_2 \dots j_n} \, |1\rangle\right)}{2^{n/2}}
\end{aligned}
$$


$|j_1\rangle$
$|j_2\rangle$
$|j_{n-1}\rangle$
$|j_n\rangle$
H
R_2
R_{n-1}
R_n
H
R_{n-2}
R_{n-1}
H
R_2
H
$|0\rangle + e^{2\pi i\, 0.j_1\cdots j_n}|1\rangle$
$|0\rangle + e^{2\pi i\, 0.j_2\cdots j_n}|1\rangle$
$|0\rangle + e^{2\pi i\, 0.j_{n-1}j_n}|1\rangle$
$|0\rangle + e^{2\pi i\, 0.j_n}|1\rangle$

Applying the Hadamard gate to the first qubit of the input state $|j_1 \dots j_n\rangle$ gives

$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i\ 0.j_1}|1\rangle\right)|j_2 \dots j_n\rangle$$

since $e^{2\pi i\ 0.j_1}$ equals $+1$ when $j_1 = 0$ and equals -1 when $j_1 = 1$.
We define a unitary gate R_k as

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$$

The controlled-R_2 gate applied on the first qubit, conditional on j_2, now gives

$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i\ 0.j_1 j_2}|1\rangle\right)|j_2 \dots j_n\rangle$$

Applying further the controlled-R_3, R_4 ... R_n gates, conditional on j_3, j_4 etc., we get

$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i\ 0.j_1 j_2 \dots j_n}|1\rangle\right)|j_2 \dots j_n\rangle$$

Next we perform a similar procedure onto the second qubit. The Hadamard gate produces the state

$$\frac{1}{2^{2/2}}\left(|0\rangle + e^{2\pi i\ 0.j_1 j_2 \dots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i\ 0.j_2}|1\rangle\right)|j_3 \dots j_n\rangle$$

and the controlled-R_2 through R_n gates yield the state

$$\frac{1}{2^{2/2}}\left(|0\rangle + e^{2\pi i\ 0.j_1 j_2 \dots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i\ 0.j_2 \dots j_n}|1\rangle\right)|j_3 \dots j_n\rangle$$

We continue this procedure for each qubit, obtaining a final state

$$\frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi i\ 0.j_1 j_2 \dots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i\ 0.j_2 \dots j_n}|1\rangle\right)\dots\left(|0\rangle + e^{2\pi i\ 0.j_n}|1\rangle\right)$$

Eventually, we use the $SWAP$ operations to reverse the order of the qubits to obtain the state in the desired product form

$$\frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi i\ 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i\ 0.j_{n-1} j_n}|1\rangle\right)\dots\left(|0\rangle + e^{2\pi i\ 0.j_1 j_2 \dots j_n}|1\rangle\right)$$

Complexity of quantum Fourier transform

How many gates the circuit uses?

qubit	# of Hadamard gates	# of controlled-R gates	total # of gates
1	1	$n-1$	n
2	1	$n-2$	$n-1$
$\dots$			
$n-1$	1	1	2
n	1	0	1
Total			$n(n+1)/2$ plus $\frac{n}{2}$ $SWAP$ gates

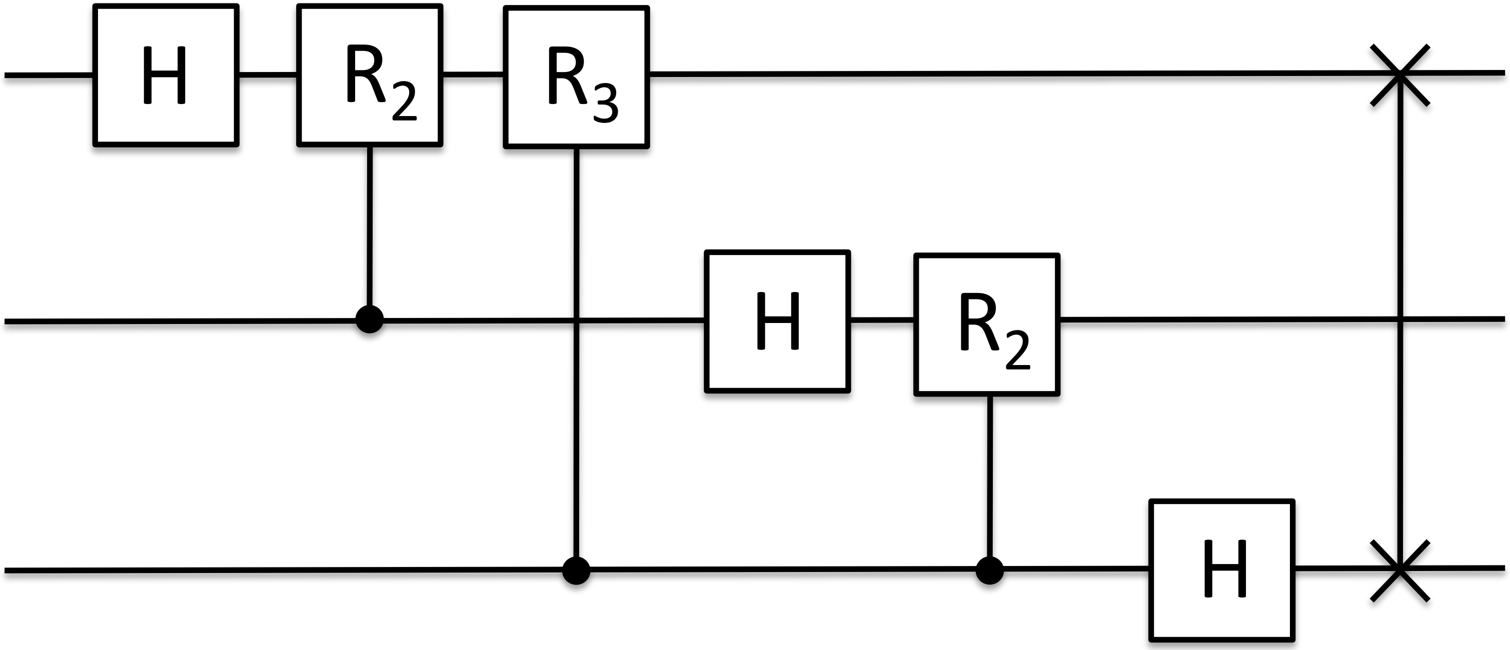
The circuit provides $\Theta(n^2)$ algorithm for performing quantum Fourier transform.

The best classical algorithms for the discrete Fourier transform, such as the Fast Fourier Transform, require $\Theta(n2^n)$ gates to perform the transform on 2^n elements.

Example: Three qubit QFT

In this case, we will need only the controlled R_2 and R_3 gates. Note that

$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i/2} \end{pmatrix} = \hat{S} \qquad R_3 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i/4} \end{pmatrix} = \hat{T}$$



The quantum Fourier transform can in this case be written explicitly as a matrix

$$QFT_3 = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{pmatrix}$$

where $\omega = e^{2\pi i/8} = \sqrt{i}$.

Quantum phase estimation subroutine

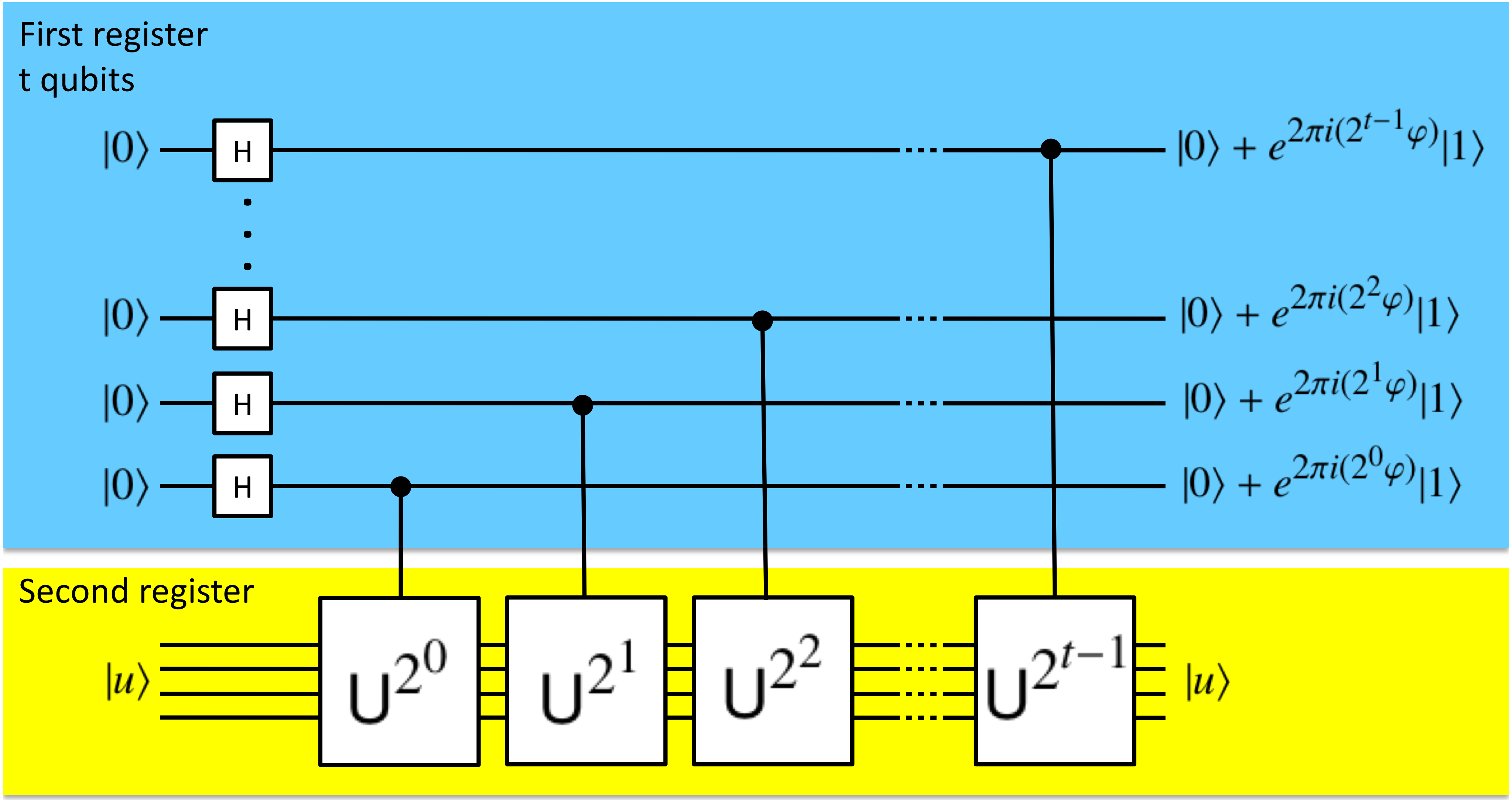
Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i\varphi}$ where the value of φ is unknown. The goal of the phase estimation algorithm is to estimate φ.

We assume that we have *black boxes*, also called *oracles*, capable of preparing the state $|u\rangle$ and performing the controlled-U^{2^j} operation for suitable nonnegative $j \in \mathbb{Z}$.

The phase estimation procedure will use two *registers*:

- the first containing t qubits in the state $|0\rangle$; t depends on the desired accuracy of the phase estimation and on the probability of it being successful.

- the second register begins in the state $|u\rangle$ and contains as many qubits as necessary to store it.


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

Quantum phase estimation circuit

The circuit begins by applying a Hadamard gates to the first register followed by the application of controlled-U operations on the second register, with U raised to successive powers of two.

The final state of the first register is

$$\begin{aligned} &\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i\ 2^{t-1}\varphi}\,|1\rangle\right)\left(|0\rangle + e^{2\pi i\ 2^{t-2}\varphi}\,|1\rangle\right)\ \ldots\ \left(|0\rangle + e^{2\pi i\ 2^{0}\varphi}\,|1\rangle\right) \\ &= \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}\,|k\rangle \end{aligned}$$

$$\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i\, 2^{t-1}\varphi}\,|1\rangle\right)\left(|0\rangle + e^{2\pi i\, 2^{t-2}\varphi}\,|1\rangle\right)\ \ldots\ \left(|0\rangle + e^{2\pi i\, 2^{0}\varphi}\,|1\rangle\right)$$

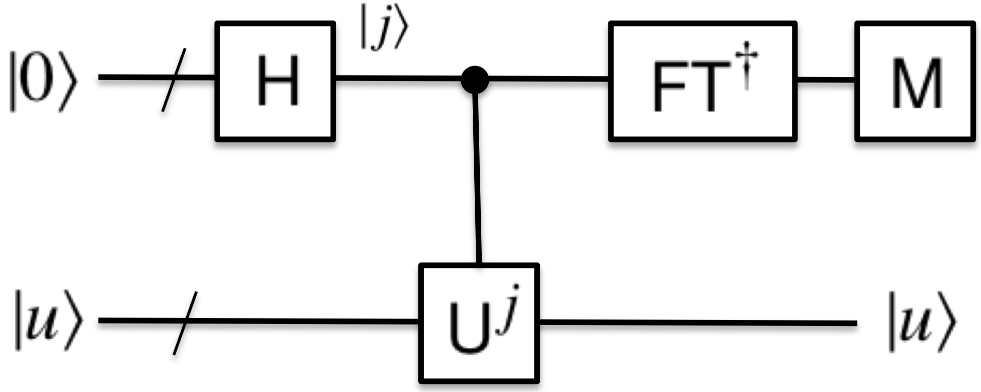
Suppose that φ can be expressed exactly in t bits as $\varphi = 0.\varphi_1 \ldots \varphi_t$. Then the final state of the first stage may be written as

$$\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i\, 0.\varphi_t}\,|1\rangle\right)\left(|0\rangle + e^{2\pi i\, 0.\varphi_{t-1}\varphi_t}\,|1\rangle\right)\ \ldots\ \left(|0\rangle + e^{2\pi i\, 0.\varphi_1\varphi_2\ldots\varphi_t}\,|1\rangle\right)$$

The second stage of the algorithm is to apply the **inverse** Fourier transform, obtained by reversing the QFT circuit, on the first register:

$$\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}\,|k\rangle\,|u\rangle \quad \rightarrow \quad |\varphi_1\varphi_2\ldots\varphi_t\rangle\,|u\rangle = |\tilde{\varphi}\rangle\,|u\rangle$$

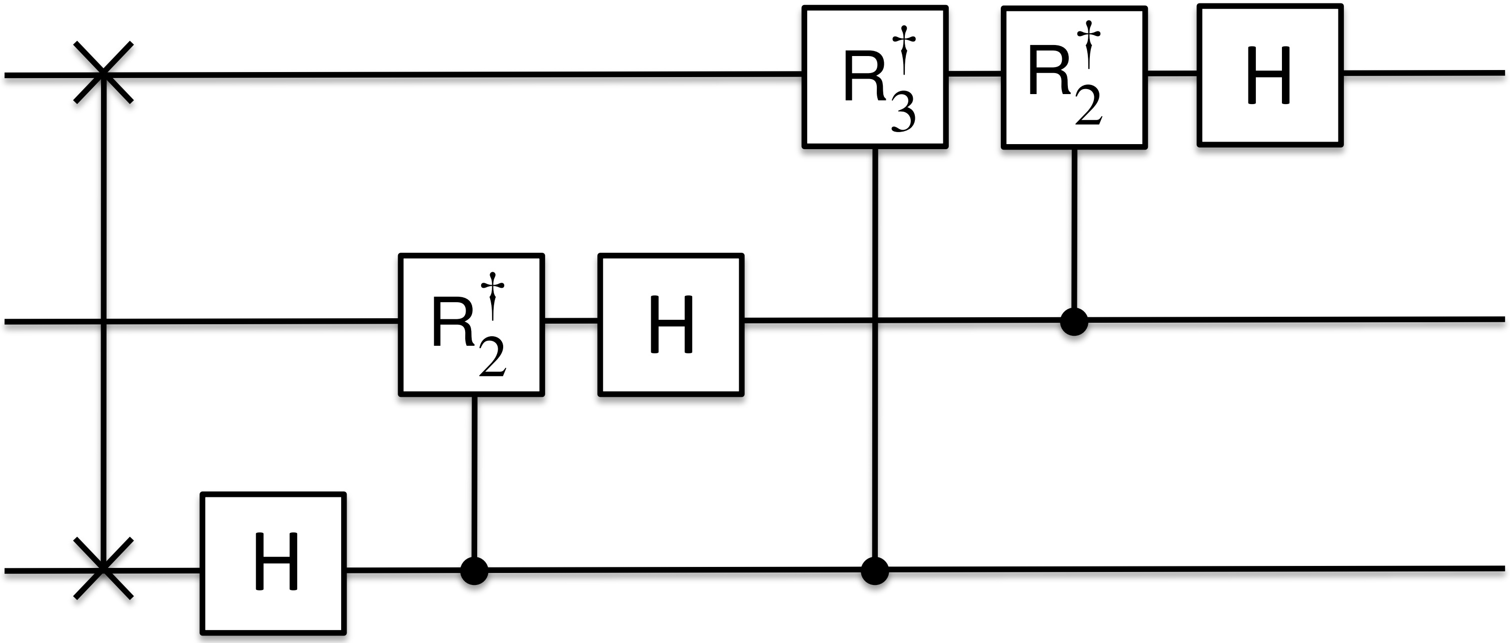
This step can be done in $\Theta(t^2)$ steps.



Example: Three qubit inverse QFT

The inverse QFT circuit is the adjoint of the circuit for QFT: QFT†

$$R_2^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{-2\pi i/2^2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{-\pi i/2} \end{pmatrix} = \hat{S}^\dagger \qquad R_3^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{-\pi i/4} \end{pmatrix} = \hat{T}^\dagger$$



The third stage is the measurement of the first register in the standard computational basis.

If φ was expressed exactly in t qubits, the measurement would give us φ exactly. In general, $|\tilde{\varphi}\rangle$ is a good estimate of the phase φ of an eigenvalue of the unitary operator U.

To successfully obtain φ accurate to n bits with probability of success at least $1 - \epsilon$, the algorithm requires

$$t = n + \left\lceil \log\left(2 + \frac{1}{2\epsilon}\right) \right\rceil$$

Applications

1. Order-finding algorithm

The order of x modulo N is the least positive integer r such that $x^r \mathrm{mod} N = 1$. This number can be computed in $O(L^3)$ operations using the quantum phase estimation algorithm, for L-bit integers x and N.

2. Factoring (Shor)

The prime factors of an L-bit integer N can be determined in $O(L^3)$ operations by reducing this problem to finding the order of a random number x co-prime with N.

3. Hidden subgroup problem

If we are given a periodic function, even when the structure of the periodicity is quite complicated, we can often use a quantum algorithm to determine the periodicity.

All the known fast quantum algorithms can be described as solving the following problem:

Let f be a function from a finitely generated group G to a finite set X such that f is constant on the cosets of a subgroup K, and distinct on each coset. Given a quantum black box for performing the unitary transform $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$, for $g \in G$ and $h \in X$, find a generating set for K.

Quantum search algorithm (Grover)

Consider an unsorted database with $N = 2^n$ entries. The algorithm requires an N-dimensional state space $\mathcal{H}$, which can be supplied by $n = \log_2 N$ qubits.

Consider the problem of determining the index of the database entry which satisfies some search criterion.

Let f be the function which maps database entries to 0 or 1, where $f(\omega) = 1$ if and only if ω satisfies the search criterion. We are provided with oracle access to a subroutine in the form of a unitary operator, U_ω, which acts as follows (for the ω for which $f(\omega) = 1$):

$$\begin{aligned} U_\omega|\omega\rangle &= -|\omega\rangle \\ U_\omega|x\rangle &= |x\rangle, \text{ for all } x \neq \omega \end{aligned}$$

Our goal is to identfy the index $|\omega\rangle$.

Algorithm

Let $|s\rangle$ denote the uniform superposition over all states

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

We introduce the operator

$$U_s = 2|s\rangle\langle s| - 1$$

known as the Grover diffusion operator.

1. Initialize the system to the state

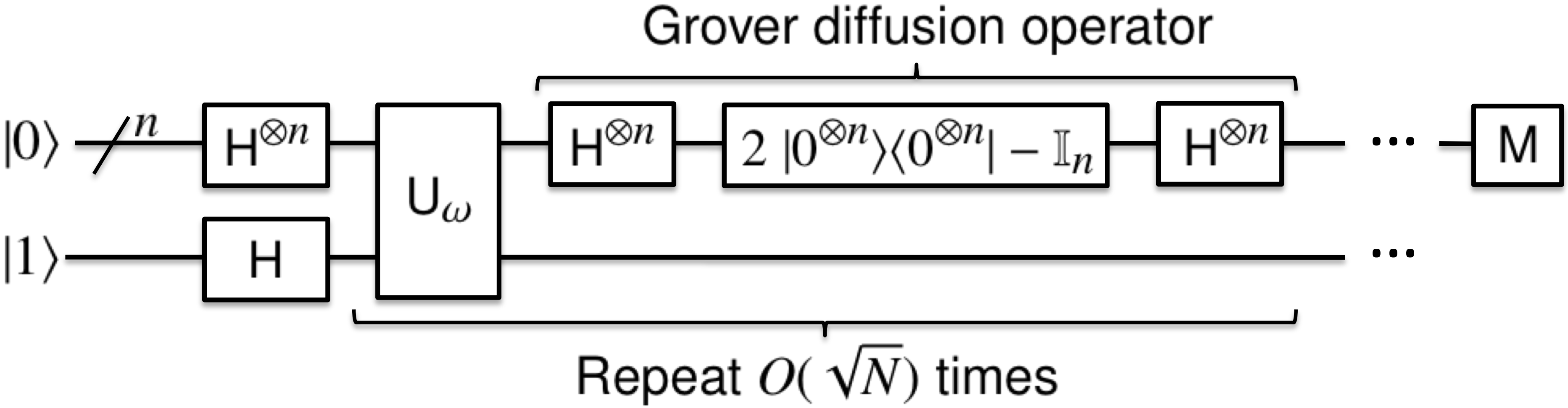
$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

2. Perform the following Grover iteration $r(N)$ times where $r(N)$ is asymptotically $O(\sqrt{N})$:

   a) apply the operator U_ω;

   b) apply the operator U_s.

3. Perform the measurement Ω. The measurement result will be λ_ω with the probability approaching 1 for $N >> 1$. From λ_ω, ω may be obtained.


Grover diffusion operator
$|0\rangle$
n
$\mathrm{H}^{\otimes n}$
U_ω
$\mathrm{H}^{\otimes n}$
$2\,|0^{\otimes n}\rangle\langle 0^{\otimes n}| - \mathbb{I}_n$
$\mathrm{H}^{\otimes n}$
...
M
$|1\rangle$
H
...
Repeat $O(\sqrt{N})$ times

Consider the plane spanned by $|s\rangle$ and $|\omega\rangle$, or equivalently the plane spanned by $|\omega\rangle$ and

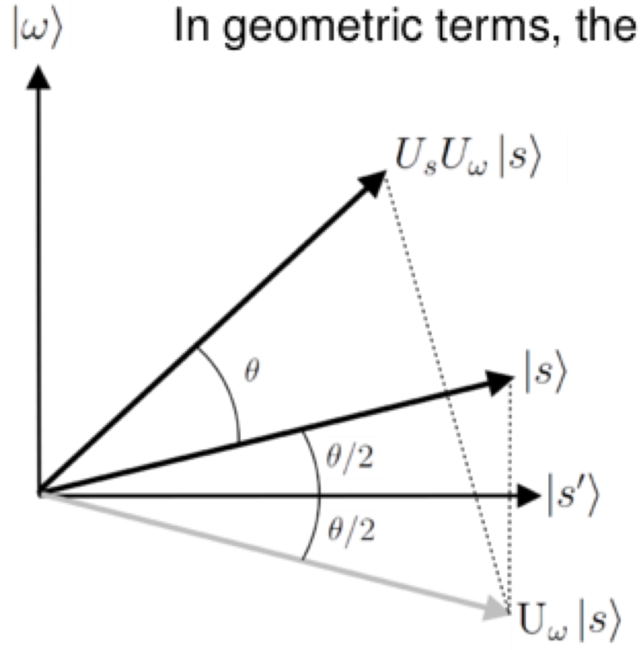
$$|s'\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq \omega} |x\rangle$$

We will consider the first iteration, acting on the initial ket $|s\rangle$. Since $|\omega\rangle$ is one of the basis vectors in $|s\rangle$ the overlap

$$\langle s'|s\rangle = \sqrt{\frac{N-1}{N}}$$

In geometric terms, the angle between $|s\rangle$ and $|s'\rangle$ is given as

$$\sin\theta/2 = \frac{1}{\sqrt{N}}$$

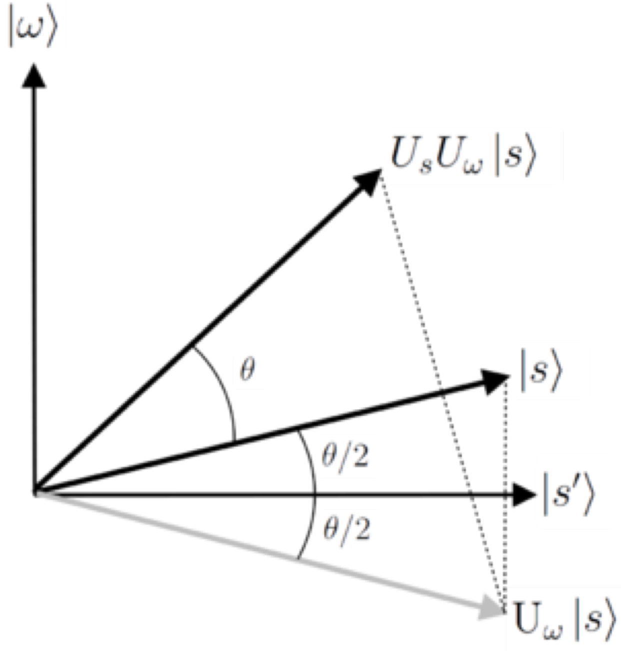


The operator U_ω is a reflection at the hyperplane orthogonal to $|\omega\rangle$ for vectors in the plane spanned by $|\omega\rangle$ and $|s'\rangle$, that is it acts as a reflection across $|s'\rangle$.

The operator U_s is a reflection through $|s\rangle$. Therefore, the state vector remains in the plane spanned by $|\omega\rangle$ and $|s'\rangle$ after each application of the operators U_s and U_ω.

The operator $U_s U_\omega$ of each iteration rotates the state vector by an angle

$$\theta = 2\arcsin\frac{1}{\sqrt{N}}$$



We need to stop when the state vector passes close to $|\omega\rangle$; after this, subsequent iterations rotate the state vector away from $|\omega\rangle$, reducing the probability of obtaining the correct answer.

The exact probability of measuring the correct answer is:

$$\sin^2\left(\left(r + \frac{1}{2}\right)\theta\right)$$

where r is the number of Grover iterations.

The earliest time we get the near-optimal measurement is $r \approx \pi\sqrt{N}/4$.