1 Quantum Fourier transform and phase estimation

The quantum Fourier transform is a component of a number of quantum algorithms, the Shor factoring algorithm in particular. We will not treat the Shor algorithm in this book, as it has been covered extensively in many other places. We will show instead how the quantum Fourier transform can be used to find an unknown eigenvalue of a unitary transformation.

Let $|a\rangle$ be a member of the computational basis in the m-qubit Hilbert space. The m-bit binary number a can be expressed as $a = 2^{m-1}a_1 + 2^{m-1}a_2 + \ldots + 2^0 a_m$, where each of the a_j are either 0 or 1. The quantum Fourier transform, U_F, takes $|a\rangle$ into the state

$$U_F|a\rangle = \frac{1}{2^m}\sum_{y=0}^{2^m-1} e^{2\pi i a\cdot y/2^m}|y\rangle. \tag{1}$$

The inverse transformation is given by

$$U_F^{-1}|a\rangle = \frac{1}{2^m}\sum_{y=0}^{2^m-1} e^{-2\pi i a\cdot y/2^m}|y\rangle. \tag{2}$$

This transformation can implemented efficiently using only one and two-qubit gates.

Now let us see how we can use the quantum Fourier transform to estimate an unknown eigenvalue. Suppose that we have the unitary operator U, where $U|\psi\rangle = \exp(2\pi i\phi)|\psi\rangle$ and $0 \leq \phi < 1$. We are given one copy of $|\psi\rangle$ and gates that perform Controlled-U^k operations for $k = 1, 2, 2^2, \ldots 2^{m-1}$. We want to find ϕ, which we do not know, to m-bit accuracy. We start with each of the qubits in the m control lines in the state $(|0\rangle + |1\rangle)/\sqrt{2}$, so that the initial state of our computation is

$$2^{-m/2}[\prod_{j=0}^{m-1}(|0\rangle_j + |1\rangle_j)] \otimes |\psi\rangle. \tag{3}$$

We now apply the Controlled-U^{2^j} gates, the control being the j^{th} qubit and the target being the system in the state $|\psi\rangle$. This results in the state

$$2^{-m/2}[\prod_{j=0}^{m-1}(|0\rangle_j + e^{2\pi i 2^j\phi}|1\rangle_j)] \otimes |\psi\rangle = 2^{-m/2}\sum_{y=0}^{2^m-1} e^{2\pi i\phi y}|y\rangle \otimes |\psi\rangle, \tag{4}$$

where $|y\rangle$ is an m-qubit computational basis state. Now if ϕ is of the form $a/2^m$, where a is an m-digit binary number, we can simply apply the inverse quantum Fourier transform to the above state, and the result will be $|a\rangle$. We will then have learned ϕ.

Now let us see what happens if ϕ is not of the form $a/2^m$. Let $\phi = (a/2^m)+\delta$, where a is the closest m-bit binary number to $2^m\phi$. This implies that $0 < |\delta| \leq 2^{-(m+1)}$. We now apply the inverse Fourier transform to the state in Eq. (4) yielding

$$2^{-m}\sum_{y=0}^{2^m-1}\sum_{x=0}^{2^m-1} e^{-2\pi i x\cdot y/2^m} e^{2\pi i\phi y}|x\rangle = 2^{-m}\sum_{y=0}^{2^m-1}\sum_{x=0}^{2^m-1} e^{2\pi i(a-x)\cdot y/2^m} e^{2\pi i\delta y}|x\rangle, \tag{5}$$

where we have dropped $|\psi\rangle$ since it is not entangled with the rest of the state and plays no further role. Now let us look at the coefficient of the state $|a\rangle$ in the above equation. It is given by

$$2^{-m}\sum_{y=0}^{2^m-1} e^{2\pi i\delta y} = 2^{-m}\left(\frac{1-e^{2\pi i\delta 2^m}}{1-e^{2\pi i\delta}}\right). \tag{6}$$

We now want to bound the magnitudes of the numerator and denominator of this fraction. In order to do so we note that

$$|1-e^{i\theta}| = \sqrt{2}(1-\cos\theta)^{1/2} = 2\sin(\theta/2). \tag{7}$$

Now for $0 \leq \beta \leq \pi/2$, we have that $(2/\pi)\beta \leq \sin\beta \leq \beta$. Setting $\beta = \theta/2$ we have that for $0 \leq \theta \leq \pi$,

$$\frac{2\theta}{\pi} \leq |1-e^{i\theta}| \leq \theta. \tag{8}$$

Note that because $|1-e^{i\theta}| = |1-e^{-i\theta}|$, the above inequalities can be modified to hold in the range $-\pi \leq \theta \leq \pi$ by inserting absolute value signs appropriately

$$\frac{2|\theta|}{\pi} \leq |1-e^{i\theta}| \leq |\theta|. \tag{9}$$

Now because $|\delta| \leq 1/2^{m+1}$, we have that $2\pi\delta 2^m \leq \pi$ and, therefore, $|1-e^{2\pi i\delta 2^m}| \geq 4\delta 2^m$, and we also have that $|1-e^{2\pi i\delta}| \leq 2\pi\delta$. This implies that the probability of obtaining the state $|a\rangle$ when measuring the output state of the circuit is

$$2^{-2m}\left|\frac{1-e^{2\pi i\delta 2^m}}{1-e^{2\pi i\delta}}\right|^2 \geq 2^{-2m}\left(\frac{4\delta 2^m}{2\pi\delta}\right)^2 = \frac{4}{\pi^2}. \tag{10}$$

Therefore, the probability of obtaining the best m-bit approximation to ϕ is $(4/\pi^2) = 0.4$. A more detailed analysis shows that the probability of getting an error greater than $k/2^m$ is less than $1/(2k-1)$.

One possible use for this algorithm is related to the Grover search. Suppose we are given a black box Boolean function that is of one of two types. There is either one input, x_0, which we do not know, for which $f(x_0) = 1$, with all other inputs, $x \neq x_0$ yielding $f(x) = 0$, or all inputs yield $f(x) = 0$. We would like to find which type of black box function we have. One approach is to run the Grover algorithm and see if we get the same answer almost all of the time.

If so, they we have the first kind of black box. If we get different answers each time, then we have the second type. A second approach is to use the phase estimation algorithm. The operator $Q = U_{w_0^\perp} U_f$ has different eigenvalues for the two different types of oracles. In the case that all inputs yield $f(x) = 0$, we have that $U_f = I$, which implies that $Q = U_{w_0^\perp}$. In that case, Q is just a reflection, so that its eigenvalues are just ± 1. In particular, the state $|w_0\rangle$ is an eigenstate with eigenvalue 1. If one of the inputs yields $f(x_0) = 1$, then in the subspace S', Q can be expressed as a 2×2 matrix in the $\{|w_0\rangle, |w_0^\perp\rangle\}$ basis

$$Q = \begin{pmatrix} \cos 2\alpha & -\sin 2\alpha \\ \sin 2\alpha & \cos 2\alpha \end{pmatrix}, \tag{11}$$

where α is the angle between $|w_0\rangle$ and $|x_0^\perp\rangle$ and is $O(N^{-1/2})$. This matrix has eigenvalues $e^{\pm 2i\alpha}$, and the eigenstates are $|\alpha_\pm\rangle = (|w_0\rangle \mp i|w_0^\perp\rangle)/\sqrt{2}$. Now suppose that N, the number of possible inputs to our Boolean function is $N = 2^n$. In order to discriminate between the two types of oracles, we need to determine the eigenvalues of Q to $O(2^{-n/2})$, because $1 - e^{2i\alpha}$ is of this order. We then make use of the phase estimation algorithm with $m > n/2$ and an input state into the target qubits of the Controlled-Q^{2^j} gates of $|w_0\rangle$. Now $|w_0\rangle$ is not an eigenstate of Q, but it is the sum of two eigenstates $|w_0\rangle = (|\alpha_+\rangle + |\alpha_-\rangle)/\sqrt{2}$. The output of the phase estimation circuit will be approximately of the form $(|a_+\rangle|\alpha_+\rangle + |a_-\rangle|\alpha_-\rangle)/\sqrt{2}$ where $a_+/2^m$ is a good estimate of $\alpha/2\pi$ and $a_-/2^m$ is a good estimate of $(2\pi - \alpha)/2\pi$. If we simply measure the first m qubits of the output state in the computational basis, we will obtain, with equal probability an estimate of either a_+ or a_-. If either one of these is different from zero, then the we know that there is an x_0 such that $f(x_0) = 1$.

The procedure we have just outlined is most useful when there is more than one value of x such that $f(x) = 1$, and we want to find out how many values of x satisfying this condition there are. This is a procedure known as quantum counting. In that case the eigenvalues of Q depend on the number of solutions, and by estimating the eigenvalues we can determine that number.

2 Quantum walks

Finding new quantum algorithms has not been easy, and one approach one might try to find new ones is to see if there are particular mathematical structures that have proved useful in classical algorithms and then try to generalize them to the quantum realm. One area in which this approach has been fruitful is in algorithms based on random walks. There are a number of classical algorithms based on random walks, and we shall present an example of one shortly. It has been possible to define a quantum version of a random walk, known as a quantum walk, and there are now new quantum algorithms that are based on quantum walks. In this section we will describe what a quantum walk is and some of the things they can do.

The simplest example of a classical random walk is one on a line. The walk starts at a point, which we shall call the origin. The walker then flips an unbiased coin. If it comes up heads, he takes one step to the right, if tails, one step to the left (all steps are the same length). This process is repeated for the desired number of steps, n. The result can be described by a probability distribution, $p(x;n)$, which is the probability of being at position x after n steps. The position is measured in units of step length, and is positive to the right of the origin (which is $x=0$) and negative to the left. For example, for a walk of two steps, the only possible final positions are $x=-2,0,2$ and we find that $p(-2;2)=p(2;2)=1/4$ and $p(0;2)=1/2$.

It is also possible to perform random walks on more general structures known as graphs. A graph consists of a set of vertices, V, and a set of edges, E. Each edge connects two of the vertices, and an edge is labelled by an unordered pair of vertices, which are just the vertices connected by that edge. In general, not all of the vertices will be connected by an edge. A graph in which each pair of vertices is connected by an edge is known as a complete graph, and if there are N vertices, there will be $N(N-1)/2$ edges in a complete graph. In order to perform a random walk on a graph, we choose one vertex on which to start. For the first step, we see which vertices are connected to the vertex we are on by an edge, and then we randomly choose one of them, each having the same probability, and then move to that vertex. So, for example, if our starting vertex is connected to three other vertices, then we would end up on each of those vertices with a probability of 1/3. We then repeat this process for the new vertex in order to make the second step, and keep repeating it for as many steps as we wish.

A simple example of an algorithm based on a random walk is one that determines whether two vertices in a graph are connected or not. In order to determine whether there is a a path connecting a specified vertex u to another specified vertex v, we can start a walker at u, execute a random walk for a certain number of steps, and see after each step whether we have reached v. It can be shown that if the graph has N vertices, and we run the walk for $2N^3$ steps, then the probability of not reaching v if there is a path from u to v is less than one half. So if we run a walk of this length m times, and do not reach v during any of these walks, the probability of this occurring if there is a path from u to v is less than $1/2^m$. Therefore, we shall say that if during one of these walks we find v, then there is a path from u to v, and if after m walks of length $2N^3$ during which we do not reach v, then there is no path from u to v. Our probability of making a mistake is less than $2{-}m$. This gives us a probabilistic algorithm for determining whether there is a path from u to v.

There are a number of different ways to define a quantum walk, but we shall only explore one of them, known as the scattering quantum walk. In this walk, the particle resides on the edges and can be though of as scattering when it goes through a vertex. In particular, suppose and edge connects vertices v_1 and v_2. There are two states corresponding to this edge, and these states are assumed to be orthogonal. There is the state $|v_1v_2\rangle$ which corresponds to the particle being on the edge and going from vertex v_1 to v_2, and the state $|v_2,v_1\rangle$, which corresponds to the particle being on the edge and going from v_2 to v_1. The set of these states for all of the edges form an orthonormal basis for the Hilbert space of the walking particle.

Next we need a unitary operator that will advance the walk one time step. We obtain this operator by combining the action of local unitaries that describe what happens at the individual vertices. Let us consider a vertex v, and let ω_v be the linear span of the set of edge states entering v and Ω_v be the span of the set of edge states leaving v. Because each edge attached to v has two states, one entering and one leaving v, ω_v and Ω_v have the same dimension. The local unitary, U_v at v maps ω_v to Ω_v. We are going to require that the action of U_v be completely symmetric, that is we want it to act on all of the edges in the same way. In particular, suppose there are n edges attached to v. We want the amplitude for the particle to be reflected back onto the edge from which it entered v to be $-r$ and the amplitude for it to be transmitted through the vertex and leave by a different edge to be t. That is, if we denote the vertices attached to v by $1, 2, \ldots n$, and if the particle enters v from vertex j, then

$$U_v|j,v\rangle = -r|v,j\rangle + t\sum_{k=1,k\neq j}^{n} |v,k\rangle. \tag{12}$$

In order for U_v to be unitary, we must have that the state on the right-hand side of this equation be normalized

$$|r|^2 + (n-1)|t|^2 = 1, \tag{13}$$

and that output states resulting from orthogonal input states be orthogonal

$$-r^*t - rt^* + (n-2)|t|^2 = 0. \tag{14}$$

If, for convenience, we also require that r and t be real, we find that

$$r = \frac{n-2}{n} \qquad t = \frac{2}{n}. \tag{15}$$

Note that with this choice, $r + t = 1$. The action of the unitary operator U that advances walk one step, is given by the combined action of all of the operators U_v at the different vertices.

Let us look at a walk on a simple graph known as a star graph. It consists of a central vertex with N edges attached to it and N vertices attached to the other ends of these edges. We shall denote the central vertex by 0 and the outer vertices by $1, 2, \ldots N$. The local unitary corresponding to the central vertex is described by the operator U_v above with $r = (N-2)/N$ and $t = 2/N$. The outer vertices reflect the particle except for one, which we shall assume is vertex 1, that reflects the particle and flips the phase of the state as well. That is the marked vertex, the one that is different from the others, that we are trying to find. Therefore, we have $U|0,j\rangle = |j,0\rangle$ for $j \geq 2$ and $U|0,1\rangle = -|1,0\rangle$. We shall start the walk in the state

$$|\psi_{init}\rangle = \frac{1}{\sqrt{N}}\sum_{j=1}^{N} |0,j\rangle. \tag{16}$$

Because of the symmetry of the problem the walk takes place in a only a subspace of the entire Hilbert space, and the dimension of this subspace is small. In particular, if we define

$$\begin{aligned} |\psi_1\rangle &= |0,1\rangle \\ |\psi_2\rangle &= |1,0\rangle \\ |\psi_3\rangle &= \frac{1}{\sqrt{N-1}}\sum_{j=2}^{N}|0,j\rangle \\ |\psi_4\rangle &= \frac{1}{\sqrt{N-1}}\sum_{j=2}^{N}|j,0\rangle \end{aligned} \tag{17}$$

then the action of U on these states is given by

$$\begin{aligned} U|\psi_1\rangle &= -|\psi_2\rangle \\ U|\psi_2\rangle &= -r|\psi_1\rangle + t\sqrt{N-1}|\psi_3\rangle \\ U|\psi_3\rangle &= |\psi_4\rangle \\ U|\psi_4\rangle &= r|\psi_3\rangle + t\sqrt{N-1}|\psi_1\rangle. \end{aligned} \tag{18}$$

From this we see that the four-dimensional subspace spanned by these vectors is invariant under U. Our initial state, which can be expressed as

$$|\psi_{init}\rangle = \frac{1}{\sqrt{N}}|\psi_1\rangle + \sqrt{\frac{N-1}{N}}|\psi_3\rangle, \tag{19}$$

is also in this subspace, and so the entire quantum walk will take place in the four-dimensional invariant subspace. This drastically simplifies finding the state of the particle after n steps.

Now from the way this walk has been set up, you might suspect that it will simply mimic the action of the Grover algorithm. If that is the case, you are right. In order to see this, we first note that the action of U in the invariant subspace can be described by a 4×4 matrix

$$M = \begin{pmatrix} 0 & -r & 0 & t\sqrt{N-1} \\ -1 & 0 & 0 & 0 \\ 0 & t\sqrt{N-1} & 0 & r \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{20}$$

where the matrix elements of M are given by $M_{jk} = \langle\psi_j|U|\psi_k\rangle$. In order to find out how the walk behaves, we first find the eigenvalues and eigenvectors of U. The characteristic equation for the eigenvalues, λ, of M is

$$\lambda^4 - 2r\lambda^2 + 1 = 0. \tag{21}$$

We will solve the equation in the large N limit. In that case, we express the equation as

$$\lambda^4 - 2\lambda^2 + 1 + 2t\lambda^2 = 0. \tag{22}$$

We ignore the last term on the left-hand side, which is small when N is large, in order to find zeroth order solutions, λ_0. This gives $\lambda_0 = \pm 1$. We now set $\lambda = \lambda_0 + \delta\lambda$, and substitute it back into the equation. Keeping terms of up to second order in small quantities we find that for $\lambda_0 = 1$

$$\delta\lambda^2 + \frac{1}{2}t(1 + 2\delta\lambda) = 0, \tag{23}$$

and for $\lambda_0 = -1$ we find

$$\delta\lambda^2 + \frac{1}{2}t(1 - 2\delta\lambda) = 0. \tag{24}$$

In both cases, the solutions are, to lowest order in $1/N$

$$\delta\lambda = \pm i\sqrt{\frac{t}{2}}, \tag{25}$$

which is of order $N^{-1/2}$.

It is also necessary to find the eigenstates of M. Setting $\Delta = \sqrt{t/2}$, we have that for $\lambda = 1 + i\Delta$ and $\lambda = 1 - i\Delta$, the eigenstates are, respectively,

$$|u_1\rangle = \frac{1}{2}\begin{pmatrix} -1 \\ 1 \\ -i \\ -i \end{pmatrix} \qquad |u_2\rangle = \frac{1}{2}\begin{pmatrix} -1 \\ 1 \\ i \\ i \end{pmatrix}, \tag{26}$$

and for $\lambda = -1 + i\Delta$ and $\lambda = -1 - i\Delta$, the eigenstates are, respectively,

$$|u_3\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ -i \\ i \end{pmatrix} \qquad |u_4\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ i \\ -i \end{pmatrix}. \tag{27}$$

In terms of the eigenstates, we see that

$$|\psi_{init}\rangle = \frac{i}{2}(|u_1\rangle - |u_2\rangle + |u_3\rangle - |u_4\rangle) + O(N^{-1/2}). \tag{28}$$

Noting that $1 \pm i\Delta \cong e^{\pm i\Delta}$ and $-1 \pm i\Delta \cong -e^{\mp i\Delta}$, we have that

$$\begin{aligned} U^n|\psi_{init}\rangle &= \frac{i}{2}[e^{in\Delta}|u_1\rangle - e^{-in\Delta}|u_2\rangle \\ &\quad +(-1)^n(e^{-in\Delta}|u_3\rangle - e^{in\Delta}|u_4\rangle)] + O(N^{-1/2}), \end{aligned} \tag{29}$$

or

$$U^n|\psi_{init}\rangle = \frac{1}{2}\begin{pmatrix} \sin(n\Delta) \\ -\sin(n\Delta) \\ \cos(n\Delta) \\ \cos(n\Delta) \end{pmatrix} + \frac{1}{2}(-1)^n \begin{pmatrix} \sin(n\Delta) \\ \sin(n\Delta) \\ \cos(n\Delta) \\ -\cos(n\Delta) \end{pmatrix}, \tag{30}$$

up to order $N^{-1/2}$.

From this result, we see that when $n\Delta$ is close to $\pi/2$, the particle will be located on the edge connected to the marked vertex. In n is even it will be in the state $|0,1\rangle$ and if n is odd it will be in the state $-|1,0\rangle$. By simply measuring the location of the particle, in particular, which edge it is on, we will find which vertex is the marked one. Note that if $n\Delta$ is close to $\pi/2$, then n is of order $\sqrt{N}$. Classically, in order to find the marked vertex, we would have to check each vertex, which would require $O(N)$ operations, whereas if we run a quantum walk, we can find the marked vertex in $O(\sqrt{N})$ steps. Therefore, we obtain a quadratic speedup.

So far, we have only used a quantum walk to do something we already knew how to do, find a marked element in a list. Let us see if we can use it to do something else. Suppose that instead of a marked vertex, our star graph has an extra edge. That is, there is an edge between two of the outer vertices, and we would like to find out where it is. A quantum walk can provide a quadratic speedup for this type of search as well.

Let's assume the extra edge is between vertices 1 and 2. That means that besides the states $|0,j\rangle$ and $|j,0\rangle$, for $j=1,2,\ldots N$, we also have the states $|1,2\rangle$ and $|2,1\rangle$. For simplicity we shall assume that vertices 1 and 2 just transmit the particle. Our unitary operator will now act as $U|0,j\rangle = |j,0\rangle$ for $j>2$, and

$$\begin{array}{ll} U|0,1\rangle = |1,2\rangle & U|0,2\rangle = |2,1\rangle \\ U|1,2\rangle = |2,0\rangle & U|2,1\rangle = |1,0\rangle . \end{array} \tag{31}$$

Its action on the states $|j,0\rangle$ is as before. The walk resulting from this choice of U can also be analyzed easily, because it stays within a five-dimensional subspace of the entire Hilbert space. Define the states

$$\begin{aligned} |\psi_1\rangle &= \frac{1}{\sqrt{2}}(|0,1\rangle + 0,2\rangle) \\ |\psi_2\rangle &= \frac{1}{\sqrt{2}}(|1,0\rangle + |2,0\rangle) \\ |\psi_3\rangle &= \frac{1}{\sqrt{N-2}}\sum_{j=3}^{N}|0,j\rangle \\ |\psi_4\rangle &= \frac{1}{\sqrt{N-2}}\sum_{j=3}^{N}|j,0\rangle \\ |\psi_5\rangle &= \frac{1}{\sqrt{2}}(|1,2\rangle + |2,1\rangle). \end{aligned} \tag{32}$$

These states span a five-dimensional space we shall call S. The unitary transformation, U, that advances the walk one step acts on these states as follows:

$$\begin{aligned} U|\psi_1\rangle &= |\psi_5\rangle \\ U|\psi_2\rangle &= -(r-t)|\psi_1\rangle + 2\sqrt{rt}|\psi_3\rangle \end{aligned}$$

$$\begin{aligned} U|\psi_3\rangle &= |\psi_4\rangle \\ U|\psi_4\rangle &= (r-t)|\psi_3\rangle + 2\sqrt{rt}|\psi_1\rangle \\ U|\psi_5\rangle &= |\psi_2\rangle. \end{aligned} \tag{33}$$

For our initial state we choose

$$\begin{aligned} |\psi_{init}\rangle &= \frac{1}{\sqrt{2N}}\sum_{j=1}^{N}(|0,j\rangle - |j,0\rangle) \\ &= \frac{1}{\sqrt{N}}(|\psi_1\rangle - |\psi_2\rangle) \\ &\quad + \sqrt{\frac{N-2}{2N}}(|\psi_3\rangle - |\psi_4\rangle), \end{aligned} \tag{34}$$

which is in S. Since the initial state is in S, and S is an invariant subspace of U, the entire walk will remain in S, and so we find ourselves in a situation similar to the previous one This search, however, is more sensitive to the choice of initial state than the previous one. While we didn't mention it before, in the previous search we could also have taken a superposition of all ingoing states instead of all outgoing ones as our initial state. In the present case, the minus sign in the first expression for initial state is essential; if it is replaced by a plus sign, the search will fail.

In order to find the evolution of the quantum state for this walk, we proceed as before and find the eigenvalues and eigenstates of U restricted to S. The matrix that describes the action of U on S is given by

$$M = \begin{pmatrix} 0 & -(r-t) & 0 & 2\sqrt{rt} & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 2\sqrt{rt} & 0 & (r-t) & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{35}$$

The characteristic equation for this matrix is

$$\lambda^5 - (r-t)\lambda^3 + (r-t)\lambda^2 - 1 = 0. \tag{36}$$

One root of this equation is $\lambda = 1$, and if we factor out $(\lambda - 1)$ from the above equation, we are left with

$$\lambda^4 + \lambda^3 + 2t\lambda^2 + \lambda + 1 = 0. \tag{37}$$

As before, we will use a perturbation expansion to find the roots of this equation with the transmission amplitude, t, as the small parameter. The zeroth order solutions are found by setting $t = 0$, which gives us the large N limit, and we find

$$\lambda^4 + \lambda^3 + \lambda + 1 = (\lambda + 1)(\lambda^3 + 1) = 0, \tag{38}$$

so the zeroth order roots are -1 twice, $e^{i\pi/3}$, and $e^{-i\pi/3}$. Setting $\lambda = -1 + \delta\lambda$, substituting into the above equation and keeping terms of up to $(\delta\lambda)^2$ gives

$$3(\delta\lambda)^2 - 4t\delta\lambda + 2t = 0, \tag{39}$$

whose solution, keeping lowest order terms is

$$\delta\lambda = \pm i\sqrt{\frac{2t}{3}} = O(N^{-1/2}). \tag{40}$$

If we set $\lambda = e^{\pm i\pi/3} + \delta\lambda$, we find that $\delta\lambda = O(N^{-1})$, so these roots and their corresponding eigenvalues are not of interest, because they will not yield a quadratic speedup.

We now need to find the eigenvectors. If the components of the eigenvectors are denoted by x_j, where $j = 1, \ldots 5$, the eigenvector equations are

$$\begin{aligned} -(r-t)x_2 + 2\sqrt{rt}x_4 &= (-1 \pm i\Delta)x_1 \\ x_5 &= (-1 \pm i\Delta)x_2 \\ 2\sqrt{rt}x_2 + (r-t)x_4 &= (-1 \pm i\Delta)x_3 \\ x_3 &= (-1 \pm i\Delta)x_4 \\ x_1 &= (-1 \pm i\Delta)x_5, \end{aligned} \tag{41}$$

where now $\Delta = (2t/3)^{1/2}$. To lowest order (the terms that were dropped are of order $1/\sqrt{N}$ or lower) the eigenvector corresponding to the eigenvalue $-1 + i\Delta$ is

$$|v_1\rangle = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ 1 \\ -i\sqrt{3/2} \\ i\sqrt{3/2} \\ -1 \end{pmatrix}, \tag{42}$$

and the eigenvector corresponding to the eigenvalue $-1 - i\Delta$ is

$$|v_2\rangle = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ 1 \\ i\sqrt{3/2} \\ -i\sqrt{3/2} \\ -1 \end{pmatrix}. \tag{43}$$

We find that, up to terms of order $N^{-1/2}$, our initial state can be expressed as

$$|\psi_{init}\rangle = \frac{i}{\sqrt{2}}(|v_1\rangle - |v_2\rangle). \tag{44}$$

Expressing the eigenvalues corresponding to $|v_1\rangle$ and $|v_2\rangle$ as

$$-1 + i\Delta \cong -e^{-i\Delta} \qquad -1 - i\Delta \cong -e^{i\Delta} \tag{45}$$

we find that the state after n steps is

$$U^n|\psi_{init}\rangle = \frac{(-1)^n}{\sqrt{3}} \begin{pmatrix} \sin(n\Delta) \\ \sin(n\Delta) \\ \sqrt{3/2}\cos(n\Delta) \\ -\sqrt{3/2}\cos(n\Delta) \\ -\sin(n\Delta) \end{pmatrix}. \tag{46}$$

From this equation, we can see that when $n\Delta = \pi/2$, the particle is located on one of the edges leading to the extra edge or on the extra edge itself. This will happen when $n = O(\sqrt{N})$.

We now need to discuss how to interpret this result. It is reasonable to assume that if we are given a graph with an extra edge in an unknown location, we only have access to the edges connecting the central vertex to the outer ones, and not to the extra edge itself (if we had access to the extra edge, then we would have to know where it is). That is, in making a measurement, we can only determine which of the edges connecting central vertex to to the outer ones the particle is on. If it is on the extra edge, we will not detect it. So, after n steps, where $n\Delta = \pi/2$, we measure the edges to which we have access to find out where the particle is. With probability $2/3$ it will be on an edge connected to the extra edge, and with probability $1/3$ it will be on the extra edge itself, in which case we won't detect it.

In comparing this procedure to a classical search for the extra edge, we shall assume that classically the graph is specified by an adjacency list, which is an efficient specification for sparse graphs. For each vertex of the graph, one lists the vertices that are connected to it by an edge. In our case, the central vertex is connected to all of the other vertices, the vertices not connected to the extra edge are connected only to the central vertex, and two of the outer vertices are connected to the central vertex and to each other. Searching this list classically would require $O(N)$ steps to find the extra edge, while the quantum procedure will succeed in $O(\sqrt{N})$ steps. Therefore, we again obtain a quadratic speedup by using a quantum walk.

We have just examined the use of quantum walks in search problems, but they have been useful in developing other types of algorithms as well. One example is element distinctness. One has a function in the form of a black box, that is one puts in an input x and the output is $f(x)$, but we have no knowledge about the function. We can only send in inputs and obtain outputs. Our task is to find two inputs, if they exist, that give the same output. This can be accomplished by using a kind of quantum walk, which requires fewer queries to the black box than is necessary on a classical computer. It is also possible to use quantum walks to evaluate certain types of Boolean formulas with fewer queries than are possible classically.

3 Problems

1. Suppose we have a star graph with a loop on one of its outer vertices, say vertex 1. The other vertices simply reflect the particle, $U|0,j\rangle = |j,0\rangle$ for $j > 1$. The loop has one quantum state, which we shall denote by $|l_1\rangle$. The unitary operator has the action $U|0,1\rangle = |l_1\rangle$ and $U|l_1\rangle = |1,0\rangle$. Show that starting with the initial state in Eq. (34) the particle making the walk will become localized on the loop and the edge connected to the loop in $O(\sqrt{N})$ steps.

2. We have a Controlled-U gate, which acts on two qubits. Qubit a is the control qubit and qubit b is the target qubit, so that $|0\rangle_a|j\rangle_b \rightarrow |0\rangle_a|j\rangle_b$ and $|1\rangle_a|j\rangle_b \rightarrow |1\rangle_a U|j\rangle_b$ for $j = 0,1$. Suppose that the eigenvalues of U are ± 1. Our task is to generate two qubits one in the $+1$ eigenstate, $|u_+\rangle$, and one in the -1 eigenstate, $|u_-\rangle$ with one use of the gate. Show, making use of the rotational invariance of the singlet state

$$|\phi_s\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle),$$

that if we start with the three-qubit state

$$|\Psi_{in}\rangle_{abc} = |+x\rangle_a|\phi_s\rangle_{bc}$$

and send qubits a and b through the Controlled-U gate and make the proper measurement of qubit a , then one of the remaining qubits will be in the state $|u_+\rangle$ and the other will be in the state $|u_-\rangle$, and we will know which qubit is in which state.

3. Suppose we have a black box that evaluates the Boolean function $f(x)$, where x is the n-bit string $x_1, x_2, \ldots x_n$. This function is a sum of linear and quadratic terms in the variables x_j and each variable appears in only one term. By considering the function $f(x) + f(\bar{x})$, where $\bar{x}$ is the n-bit string $x_1 + 1, x_2 + 1, \ldots x_n + 1$, show that we can use the Bernstein-Vazirani algorithm to determine which variables appear in quadratic terms with two function evaluations. How many evaluations would be required classically?