5.1 Exact Grover for 1 in $N$ Ordered Search

- (a) For $N = 1$ and 4, $\bar{k}$ is an integer.

<table>
<thead>
<tr>
<th>$N$</th>
<th>$\bar{k} = \frac{\pi}{4N} - \frac{1}{2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>$\frac{1}{2}$</td>
</tr>
<tr>
<td>3</td>
<td>$-\frac{1}{2} + \frac{\pi}{4\text{ArcSin}\left[\frac{1}{\sqrt{3}}\right]} \approx 0.776$</td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

- (b) In order for $B$ to be unitary, $B^\dagger B = I$. We will assume $N$ and $a$ are real and non-negative.

\[
1 = \langle 0|0 \rangle \quad (1)
\]
\[
= \langle 0|B^\dagger B|0 \rangle \quad (2)
\]
\[
= \left(\sqrt{1 - Na}\langle 0| + \sqrt{Na}\langle 1|\right) \left(\sqrt{1 - Na}\langle 0| + \sqrt{Na}\langle 1|\right) \quad (3)
\]
\[
= \|\sqrt{(1 - Na)}\|^2\langle 0|0 \rangle + \|Na\|^2\langle 1|1 \rangle \quad (4)
\]
\[
= 1 \quad (5)
\]

For this last equality to hold, $Na$ must be between 0 and 1. This can also be seen by noting that the amplitudes must give probabilities that are between 0 and 1. For instance, $\|\langle 0|B|0 \rangle\|^2 = Na$ and $\|\langle 1|B|0 \rangle\|^2 = 1 - Na$ must be between 0 and 1. Thus, $a$ should be between 0 and $\frac{1}{N}$. If $a$ were possibly negative, then $-\frac{1}{N} \leq a \leq \frac{1}{N}$.

- (c) Symmetry suggests

\[
B|1 \rangle = -\sqrt{Na}\langle 0| + \sqrt{1 - Na}\langle 1| \quad (6)
\]

We then check

\[
1 = \langle 1|1 \rangle \quad (7)
\]
\[
= \left(-\sqrt{Na}\langle 0| + \sqrt{1 - Na}\langle 1|\right) \left(-\sqrt{Na}\langle 0| + \sqrt{1 - Na}\langle 1|\right) \quad (8)
\]
\[
= Na\langle 0|0 \rangle + (1 - Na)\langle 1|1 \rangle \quad (9)
\]
\[
= 1 \quad (10)
\]

and

\[
0 = \langle 0|1 \rangle \quad (11)
\]
\[
= \left(-\sqrt{Na}\langle 0| + \sqrt{1 - Na}\langle 1|\right) \left(\sqrt{1 - Na}\langle 0| + \sqrt{Na}\langle 1|\right) \quad (12)
\]
\[
= -\sqrt{Na}\sqrt{1 - Na}\langle 0|0 \rangle + \sqrt{Na}\sqrt{1 - Na}\langle 1|1 \rangle \quad (13)
\]
\[
= 0 \quad (14)
\]

That $\langle 1|0 \rangle = 0$ follows from this last result.
• (d) Calculating explicitly (and using $W|0\rangle^\otimes n = \sqrt{1 - 1/N}|w^\perp\rangle + \sqrt{1/N}|w\rangle$ from earlier in the problem)

$$W'|0\rangle^\otimes(n+1) = B \otimes H^\otimes n |0\rangle \otimes |0\rangle^\otimes n$$

$$= \left[ \sqrt{1 - Na}|0\rangle + \sqrt{Na}|1\rangle \right] \otimes \left[ \sqrt{1 - 1/N}|w^\perp\rangle + \sqrt{1/N}|w\rangle \right]$$

$$= \sqrt{(1 - Na)(1 - 1/N)}|0\rangle|w^\perp\rangle + \sqrt{Na - a}|1\rangle|w^\perp\rangle + \sqrt{1/N - a}|0\rangle|w\rangle$$

$$= \cos \alpha'|w^\perp\rangle + \sin \alpha'|w\rangle$$

where we have simply lumped the terms orthogonal to $|w\rangle^\prime = |0\rangle|w\rangle$ into an orthogonal term $|w^\perp\rangle^\prime$ with the appropriate phase.

• (e) We write

$$Z_X' = I - 2|w\rangle\langle w^\prime| = I - 2|1\rangle\langle 1| \otimes |w\rangle\langle w|$$

If the first qubit is in the state $|0\rangle$, then $Z_X' = I$. If it is in state $|1\rangle$, then $Z_X'$ performs $Z_X$ on the remaining qubits. By definition, this is the controlled gate, $\Lambda(Z_X)$.

• (f) Using the definitions given in the problem, we calculate

$$a = \sin^2 \alpha' = \sin^2 \frac{\pi}{4[\bar{k}] + 2} \leq \sin^2 \frac{\pi}{4[\bar{k}] + 2} = \sin^2 \alpha$$

$$= \frac{1}{N}$$

• (g) In order to yield $|w\rangle^\prime$ with certainty, we need $\sin((2k+1)\alpha') = 1$ or $(2k+1)\alpha' = \pi/2$. Setting $k = \lceil \bar{k} \rceil$, we find

$$\frac{(2\lceil \bar{k} \rceil + 1)\pi}{4\lceil \bar{k} \rceil + 2} = \frac{(2\lceil \bar{k} \rceil + 1)\pi}{2(2\lceil \bar{k} \rceil + 1)} = \frac{\pi}{2}$$

5.2 The phase estimation algorithm

• (a) At the beginning of round $j$, the input state is $|0\rangle|u\rangle$. Passing through the first Hadamard gives

$$\frac{1}{\sqrt{2}} [ |0\rangle + |1\rangle ] |u\rangle$$
The controlled $U^{2k_j}$ gate gives the state

$$\frac{1}{\sqrt{2}} \left[ |0\rangle + \exp(2\pi i \phi 2^{k_j}) |1\rangle \right] |u\rangle$$

(28)

Since the $|u\rangle$ can be factored out for the rest of the circuit, we omit it for the rest of the calculation. Noting that $\exp(-i\theta Z/2)|0\rangle = \exp(-i\theta/2)|0\rangle$ and $\exp(-i\theta Z/2)|1\rangle = \exp(i\theta/2)|1\rangle$, we find

$$e^{-i\theta_j Z/2} \frac{1}{\sqrt{2}} \left[ |0\rangle + \exp(2\pi i \phi 2^{k_j}) |1\rangle \right]$$

(29)

$$= \frac{1}{\sqrt{2}} \left[ e^{-i\theta_j/2} |0\rangle + \exp(2\pi i \phi 2^{k_j} + i\theta_j/2) |1\rangle \right]$$

(30)

$$= \frac{1}{\sqrt{2}} \left[ |0\rangle + \exp(2\pi i \phi 2^{k_j} + i\theta_j) |1\rangle \right]$$

(31)

(32)

where in the last step we have factored out an irrelevant overall phase $e^{-i\theta_j/2}$. The second Hadamard transforms the state to

$$\frac{1}{\sqrt{2}} \left[ H|0\rangle + \exp(2\pi i \phi 2^{k_j} + i\theta_j) H|1\rangle \right]$$

(33)

$$= \frac{1}{2} \left[ |0\rangle + |1\rangle + \exp(2\pi i \phi 2^{k_j} + i\theta_j) (|0\rangle - |1\rangle) \right]$$

(34)

$$= \frac{1}{2} \left[ (1 + \exp(2\pi i \phi 2^{k_j} + i\theta_j)) |0\rangle + (1 - \exp(2\pi i \phi 2^{k_j} + i\theta_j)) |1\rangle \right]$$

(35)

The probability of measuring $z_j$ is given by the norm of the coefficient of each $|j\rangle$ term above. Thus the probabilities are

$$P(z_j = 0) = \frac{1}{4} \left| 1 + \exp \left[ i(2\pi \phi 2^{k_j} + \theta_j) \right] \right|^2$$

(36)

$$P(z_j = 1) = \frac{1}{4} \left| 1 - \exp \left[ i(2\pi \phi 2^{k_j} + \theta_j) \right] \right|^2$$

(37)

- (b) Recall that

$$\phi = 0.\phi_1 \phi_2 \ldots \phi_n = \frac{1}{2} \phi_1 + \frac{1}{2^2} \phi_2 + \ldots + \frac{1}{2^n} \phi_n$$

(38)

Taking $k_1 = n - 1$, we have

$$2^{n-1} \phi = \phi_1 \phi_2 \ldots \phi_{n-1} \phi_n$$

(39)

Expanding the exponent into products, we have

$$\left( \prod_{m=1}^{n-1} e^{i2^{n-m} \pi \phi_m} \right) e^{i\pi \phi_n + i\theta_1}$$

(40)
Setting $\theta_1 = 0$, the probabilities are then

$$P(z_1 = 0) = \frac{1}{4} \|1 + \exp [i\pi \phi_n]\|^2$$  \hspace{1cm} (41)$$

$$P(z_1 = 1) = \frac{1}{4} \|1 - \exp [i\pi \phi_n]\|^2$$  \hspace{1cm} (42)$$

So that if $\phi_n = 0$, $P(z_1 = 0)$ is one and $P(z_1 = 1)$ is zero. If $\phi_n = 1$, $P(z_1 = 0)$ is zero and $P(z_1 = 1)$ is one. Thus with probability one, $z_1 = \phi_n$.

• (c) Inspired by part (b), we proceed in a similar manner by choosing $k_2 = n - 2$ so that

$$2^{n-2} \phi = \phi_1 \phi_2 \ldots \phi_{n-2} \phi_{n-1} \phi_n$$  \hspace{1cm} (43)$$

Expanding the exponent into products again, we have

$$\left( \prod_{m=1}^{n-2} e^{i2^{n-m-1} \pi \phi_m} \right) e^{i\pi \phi_{n-1} + i \frac{\pi}{2} \phi_n + i \theta_1}$$  \hspace{1cm} (44)$$

Since we know $\phi_n$ with certainty, we choose $\theta_1 = -\frac{\pi}{2} \phi_n$, giving probabilities

$$P(z_2 = 0) = \frac{1}{4} \|1 + \exp [i\pi \phi_{n-1}]\|^2$$  \hspace{1cm} (45)$$

$$P(z_2 = 1) = \frac{1}{4} \|1 - \exp [i\pi \phi_{n-1}]\|^2$$  \hspace{1cm} (46)$$

As in part (b), these yield $z_2 = \phi_{n-1}$ with certainty.

• (d) Given the last two steps, the general procedure is as follows. On step $j$, choose $k_j = n - j$ so that

$$2^{n-j} \phi = \phi_1 \phi_2 \ldots \phi_{n-j} \phi_{n-j+1} \ldots \phi_n$$  \hspace{1cm} (47)$$

Expanding the exponent into products again, we have

$$\left( \prod_{m=1}^{n-j} e^{i2^{n-m-(j-1)} \pi \phi_m} \right) \exp \left[ i\pi \phi_{n-j+1} + i \frac{\pi}{2} \phi_{n-j+2} + \ldots + i \frac{\pi}{2^{1-j}} \phi_n + i \theta_j \right]$$  \hspace{1cm} (48)$$

Since we know $\phi_{n-j+2}$ through $\phi_n$ at stage $j$, we choose

$$\theta_j = -\pi \left[ \frac{\phi_{n-j+2}}{2} + \frac{\phi_{n-j+3}}{2^2} + \ldots + \frac{\phi_n}{2^{1-j}} \right]$$  \hspace{1cm} (49)$$

to cancel out all but the $\phi_{n-j+1}$ exponential. This gives probabilities

$$P(z_j = 0) = \frac{1}{4} \|1 + \exp [i\pi \phi_{n-j+1}]\|^2$$  \hspace{1cm} (50)$$

$$P(z_j = 1) = \frac{1}{4} \|1 - \exp [i\pi \phi_{n-j+1}]\|^2$$  \hspace{1cm} (51)$$

so that $z_j = \phi_{n-j+1}$ with certainty.