Problem 1. Searching a small quantum phonebook

(a) Consider the general case where there are $N$ entries in the phonebook. The probability that you find your friend’s name on the first lookup is $p_1 = \frac{1}{N}$. The probability of finding it on the second lookup is

$$p_2 = \left(\frac{N-1}{N}\right) \left(\frac{1}{N-1}\right) = \frac{1}{N}$$

since this involves picking any of the $N-1$ incorrect entries the first time, and then picking the correct one among the $N-1$ remaining entries the second time. Similarly,

$$p_3 = \left(\frac{N-1}{N}\right) \left(\frac{N-2}{N-1}\right) \left(\frac{1}{N-2}\right) = \frac{1}{N}$$

and in the same way,

$$p_4 = \cdots = p_{N-2} = \frac{1}{N}$$

Of course, you never need more than $N-1$ lookups. Thus,

$$p_{N-1} = 1 - \sum_{n=1}^{N-2} p_n = 1 - \frac{N-2}{N} = \frac{2}{N}$$

The average number of lookups needed is then

$$\langle n \rangle_N = \sum_{n=1}^{N-1} n p_n = \frac{1}{N} \left(\sum_{n=1}^{N-2} n + 2(N-1)\right) = \frac{1}{N} \left(\frac{(N-1)(N-2)}{2} + 2(N-1)\right) = \frac{(N-1)(N+2)}{2N}$$

Setting $N = 4$,

$$\langle n \rangle_4 = \frac{9}{4}$$

(b) When $x \neq x_0$ (that is, when $\langle x|x_0 \rangle = 0$),

$$U_{F_0} \ket{x} \ket{0} \rightarrow \ket{x} \ket{0 \oplus 0} = \ket{x} \ket{0} \quad \text{and} \quad U_{F_0} \ket{x} \ket{1} \rightarrow \ket{x} \ket{1 \oplus 0} = \ket{x} \ket{1}$$

When $x = x_0$,

$$U_{F_0} \ket{x_0} \ket{0} \rightarrow \ket{x_0} \ket{0 \oplus 1} = \ket{x_0} \ket{1} \quad \text{and} \quad U_{F_0} \ket{x_0} \ket{1} \rightarrow \ket{x_0} \ket{1 \oplus 1} = \ket{x_0} \ket{0}$$

Therefore, $U_{F_0}$ acts on the state $\ket{x} (\ket{0} - \ket{1})/\sqrt{2}$ as $\mathbb{1}$ when $x \neq x_0$, but as $-\mathbb{1}$ when $x = x_0$. In symbols,

$$U_{F_0} \ket{x} (\ket{0} - \ket{1})/\sqrt{2} \rightarrow (\tilde{U}_{F_0} \ket{x}) (\ket{0} - \ket{1})/\sqrt{2},$$

where $\tilde{U}_{F_0} = \mathbb{1} - 2 \ket{x_0} \bra{x_0}$ acts only in the computational subspace.

(c) In general, the initial state is

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

and the Grover operation is

$$\mathcal{G}_{F_0} = U_s \tilde{U}_{F_0} = (2 \ket{s} \bra{s} - 1)(\mathbb{1} - 2 \ket{x_0} \bra{x_0})$$
The state after a single iteration is therefore
\[ |\psi_1\rangle = G_{F_0} |s\rangle = (2 |s\rangle \langle s| - 1)(1 - 2 |x_0\rangle \langle x_0|) |s\rangle = |s\rangle - 4 |s\rangle |\langle x_0|s\rangle|^2 + 2 |x_0\rangle \langle x_0|s\rangle \]
\[ = \left(1 - \frac{4}{N}\right) |s\rangle + \frac{2}{\sqrt{N}} |x_0\rangle \]

For the special case \(N = 4\), we see that
\[ |\psi_1\rangle = |x_0\rangle \]
so in this case the Grover algorithm locates your friend’s name with unit probability after a single iteration.

(d) For general \(N\),
\[ G_{F_0} |x_0\rangle = U_s (-|x_0\rangle) = (2 |s\rangle \langle s| - 1)(-|x_0\rangle) = |x_0\rangle - 2 |s\rangle \langle s|x_0\rangle = |x_0\rangle - \frac{2}{\sqrt{N}} |s\rangle \]

Together with the result of part c and linearity, this yields the state after \(T = 2\) iterations:
\[ |\psi_2\rangle = G_{F_0} |\psi_1\rangle = \left(1 - \frac{4}{N}\right) G_{F_0} |s\rangle + \frac{2}{\sqrt{N}} G_{F_0} |x_0\rangle \]
\[ = \left(1 - \frac{4}{N}\right) \left[ \left(1 - \frac{4}{N}\right) |s\rangle + \frac{2}{\sqrt{N}} |x_0\rangle \right] + \frac{2}{\sqrt{N}} \left[ |x_0\rangle - \frac{2}{\sqrt{N}} |s\rangle \right] \]

For the special case \(N = 4\), the first term above vanishes, leaving
\[ |\psi_2\rangle = |x_0\rangle - |s\rangle \]

The probability of finding your friend’s name after two iterations of Grover’s algorithm is therefore
\[ P_2 = |\langle x_0|\psi_2\rangle|^2 = \left|1 - \frac{1}{2}\right|^2 = \frac{1}{4} \]

which is as bad as guessing blindly.

If we keep going, we find that \(P_3 = 1/4\), \(P_4 = 1\), and so on, with two 1/4’s following each 1. This type of cyclic behavior will always occur for any \(N\), because we are iterating a unitary transformation on a finite-dimensional Hilbert space.