4.1 Estimating the trace of a unitary matrix

Recall that using an oracle that applies the conditional unitary \( \Lambda(U) \),

\[
\Lambda(U) : \quad |0\rangle \otimes |\psi\rangle \mapsto |0\rangle \otimes |\psi\rangle,
|1\rangle \otimes |\psi\rangle \mapsto |1\rangle \otimes U|\psi\rangle
\]  

(where \( U \) is a unitary transformation acting on \( n \) qubits), we can
measure the eigenvalues of \( U \). If the state \( |\psi\rangle \) is the eigenstate \( |\lambda\rangle \) of
\( U \) with eigenvalue \( \lambda = \exp(2\pi i \phi) \), then by querying the oracle \( k \) times,
we can determine \( \phi \) to accuracy \( O(1/\sqrt{k}) \).

But suppose that we replace the pure state \( |\psi\rangle \) in eq. (1) by the max-
imally mixed state of \( n \) qubits, \( \rho = I/2^n \).

\( a) \) Show that, with \( k \) queries, we can estimate both the real part and
the imaginary part of \( \text{tr}(U)/2^n \), the normalized trace of \( U \), to
accuracy \( O(1/\sqrt{k}) \).

\( b) \) Given a polynomial-size quantum circuit, the problem of estimat-
ing to fixed accuracy the normalized trace of the unitary trans-
formation realized by the circuit is believed to be a hard problem
classically. Explain how this problem can be solved efficiently
with a quantum computer.

The initial state needed for each query consists of one qubit in the pure
state \( |0\rangle \) and \( n \) qubits in the maximally mixed state. Surprisingly,
then, the initial state of the computer that we require to run this
(apparently) powerful quantum algorithm contains only a constant
number of “clean” qubits, and \( O(n) \) very noisy qubits.

4.2 A generalization of Simon’s problem

Simon’s problem is a hidden subgroup problem with \( G = Z_2^n \) and
\( H = Z_2 = \{0, a\} \). Consider instead the case where \( H = Z_2^k \), with gen-
erator set \( \{a_i, i = 1, 2, 3, \ldots, k\} \). That is, suppose an oracle evaluates
a function
\[ f : \{0, 1\}^n \to \{0, 1\}^{n-k}, \quad (2) \]
where we are promised that \( f \) is \( 2^k \)-to-1 such that
\[ f(x) = f(x \oplus a_i) \quad (3) \]
for \( i = 1, 2, 3, \ldots, k \) (here \( \oplus \) denotes bitwise addition modulo 2). Since the number of cosets of \( H \) in \( G \) is smaller, we can expect that the hidden subgroup is easier to find for this problem than in Simon’s \( (k = 1) \) case.

Find an algorithm using \( n - k \) quantum queries that identifies the \( k \) generators of \( H \), and show that the success probability of the algorithm is greater than 1/4.

### 4.3 Finding a collision

Suppose that a black box evaluates a function
\[ f : \{0, 1\}^n \to \{0, 1\}^{n-1}. \quad (4) \]
We are promised that the function is 2-to-1, and we are to find a “collision” – values \( x \) and \( y \) such that \( f(x) = f(y) \). This problem is harder than Simon’s problem, because we are not promised that the function is periodic. Let \( N = 2^n \).

a) Describe a randomized classical algorithm that requires \( \text{SPACE} = O(\sqrt{N}) \) and that succeeds in finding a collision with high probability in \( O(\sqrt{N}) \) queries of the black box.

b) Now suppose that only \( \text{SPACE} = O(N^{1/3}) \) is available. Describe a randomized classical algorithm that finds a collision with high probability in \( O(N^{2/3}) \) queries.

c) Show that Grover’s exhaustive search algorithm can be used to find a collision in \( O(\sqrt{N}) \) quantum queries, using \( \text{SPACE} = O(1) \).

d) Describe a quantum algorithm that uses \( \text{SPACE} = O(M) \) and finds a collision in \( O(M) + O(\sqrt{N/M}) \) quantum queries. [**Hint:** First query the box \( M \) times to learn the value of \( f(x) \) for \( M \) arguments \( \{x_1, x_2, \ldots, x_M\} \), then search for \( y \) such that \( f(y) = f(x_i) \) for some \( x_i \).] Thus, if \( M \) is chosen to optimize the number of queries, the quantum algorithm uses \( \text{SPACE} = O(N^{1/3}) \) and \( O(N^{1/3}) \) quantum queries.
4.4 Quantum counting

A black box computes a function

\[ f : \{0, 1\}^n \rightarrow \{0, 1\}, \quad (5) \]

which can be represented by a binary string

\[ X = X_{N-1}X_{N-2}\cdots X_1X_0, \quad (6) \]

where \( X_i = f(i) \) and \( N = 2^n \). Our goal is to count the number \( r \) of states “marked” by the box; that is, to determine the Hamming weight \( r = |X| \) of \( X \). We can devise a quantum algorithm that counts the marked states by combining Grover’s exhaustive search with the quantum Fourier transform.

\( a \) The black box performs an \((n+1)\)-qubit unitary transformation \( U_f \) which acts on a basis according to

\[ U_f (|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus f(x)\rangle. \quad (7) \]

If the last qubit is set to the state \(|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\), then the box applies the unitary transformation \( \tilde{U}_f \) to the first \( n \) qubits, where

\[ \tilde{U}_f |x\rangle = (-1)^{f(x)}|x\rangle. \quad (8) \]

Explain how to use the box and Hadamard gates to perform \( \Lambda(\tilde{U}_f) \), the unitary \( \tilde{U}_f \) conditioned on the value of a control qubit.

\( b \) Let

\[ |\Psi_X\rangle = \frac{1}{\sqrt{r}} \sum_{j: X_j = 1} |j\rangle \quad (9) \]

denote the uniform superposition of the marked states, and let \( U_{\text{Grover}} \) denote the “Grover iteration,” which performs a rotation by the angle \( 2\theta \) in the plane spanned by \( |\Psi_X\rangle \) and

\[ |s\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N} |j\rangle, \quad (10) \]

where

\[ \sin \theta = \langle s | \Psi_X \rangle = \sqrt{\frac{r}{N}}. \quad (11) \]
Consider a unitary transformation

\[ V : |t\rangle \otimes |\Phi\rangle \rightarrow |t\rangle \otimes U_{\text{Grover}}^t |\Phi\rangle \]  \hspace{1cm} (12)

that reads a counter register taking values \( t \in \{0, 1, 2, \ldots, T-1\} \) (where \( T = 2^m \)), and then applies \( U_{\text{Grover}} \) \( t \) times. Explain how \( V \) can be implemented, calling the oracle \( T-1 \) times. [Hint: Use the binary expansion \( t = \sum_{k=0}^{m-1} t_k 2^k \) and the conditional oracle call from (a).]

c) Suppose that \( r \ll N \). Show that, by applying \( V \), performing the quantum Fourier transform on the counter register, and then measuring the counter register, we can determine \( \theta \) to accuracy \( O(1/T) \), and hence we can find \( r \) with high success probability in \( T = O(\sqrt{rN}) \) queries. Compare to the best classical protocol.