

# AP 226 - Physics Of Quantum Information

## Problem Set #2

Due date: Feb 9, 2009  
on Susan Clark's desk (Cedar Hall A9) or in pocket on Yurika  
Peterman's door

### 1 Reading

Begin the reading assignment for homework 3. A short write up will be due February 16.

### 2 Warm up

- (a) The three steps in the original Duetsch-Josza algorithm, such as entanglement, non-local phase shift and disentanglement (quantum erasure) are realized in a single step using a double entanglement in the modified D-J algorithm. Explain the above statement by referring to the actual evolution of the state vectors.
- (b) In the Shors factoring algorithm, quantum interference is performed by quantum Fourier transform without quantum erasure step. Explain why this strategy works for the Shor algorithm even though it does not for the D-J algorithm.

### 3 Quantum Algorithms

#### 3.1 Phase Query Black Box

Let  $f$  be a binary function on  $n$  qubits. We are given a so called bit-query black-box (fig. 1) performing the unitary operation :

$$|X\rangle \otimes |a\rangle \longrightarrow |X\rangle \otimes |a \oplus f(X)\rangle$$

where  $X$  is encoded in an  $n$ -qubit register and  $a$  in one ancillary qubit.

Show that the quantum circuit given in Fig. 2 can function as a phase-query black box, defined by its action on an  $n$ -qubit register:

$$|X\rangle \longrightarrow (-1)^{f(X)} |X\rangle$$

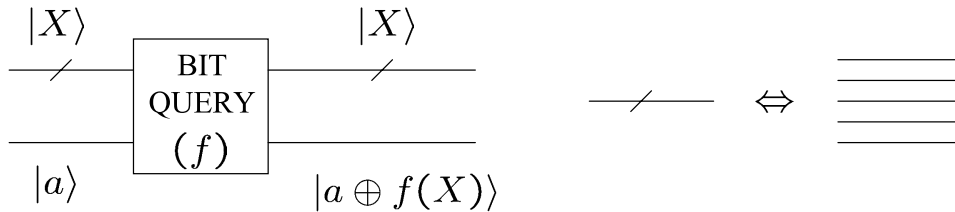


Figure 1: Bit-query black-box, acting on  $n$  register qubits plus an ancillary qubit. The upper line is crossed to indicate several qubits rather than one. This notation is common in quantum computation literature.

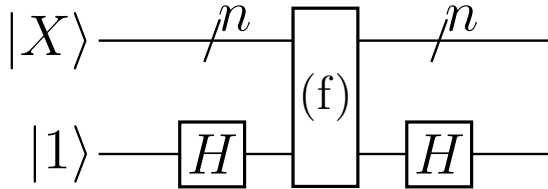


Figure 2: Phase-query quantum circuit.  $(f)$  is the bit query black box shown in Fig. 1.

### 3.2 Eigenvalue Measurement

Suppose we have a unitary operator  $U$  on  $n$  qubits. Suppose  $U$  is moreover hermitian, so that its eigenvalues are  $\pm 1$ .  $U$  can thus be seen as an observable. Show that the circuit given in Fig. 3 performs the measurement of  $U$  in a non-destructive way. This means that given an input state  $|\psi^{in}\rangle$  in our quantum register, we want to know what value  $\epsilon$  the measurement of  $U$  on  $|\psi^{in}\rangle$  will return, and leave the register in a final state  $|\psi_{\pm 1}^{out}\rangle$  which is the projection of  $|\psi^{in}\rangle$  on the appropriate eigenspace of  $U$ , corresponding its measured value.

Note that even though we measure the ancilla qubit destructively,  $\Psi$  is left in an eigenvalue of  $U$ .

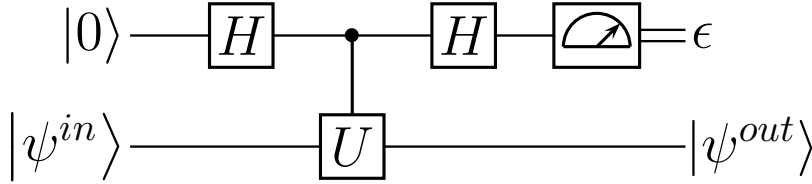


Figure 3: An eigenvalue measurement quantum circuit.

## 4 Phase Estimation Algorithm

For a general many-body system, it is hard to find the eigen-energies, as one must diagonalize a Hermitian matrix (the Hamiltonian) whose dimension is an exponential function of the number of particles. A collection of only 30 spin-1/2 particles requires the investigation of a  $2^{30}$ -dimensional Hilbert space: an overwhelming task if the system does not offer any simplifications.

In this problem, we will examine the phase-estimation algorithm, which allows a universal quantum computer to efficiently estimate the leading bits of an eigenvalue of a Hermitian operator, subject to a couple of strong restrictions. We assume that our operator of interest  $\hat{H} = \sum_{\ell} \lambda_{\ell} |\phi_{\ell}\rangle \langle \phi_{\ell}|$  acts on a Hilbert space of dimension  $2^m$ .

Refer to Figure (4). We consider a quantum computer with  $n + m$  qubits, naturally divided into two registers  $A$  and  $B$ , of  $n$  and  $m$  qubits, respectively. The orthogonal basis states of register  $A$  are  $\{|0\rangle_A, |1\rangle_A, \dots, |2^n - 1\rangle_A\}$ , and the register is initialized to the  $|0\rangle_A$  state. In this notation, the binary representation of  $a$  gives the value of each qubit for state  $|a\rangle_A$ . For example, if  $n = 3$ , then  $|0\rangle_A$  corresponds to all qubits in the logical “0” state;  $|1\rangle_A$  corresponds to the first two qubits in the logical zero state and the last qubit in the logical one

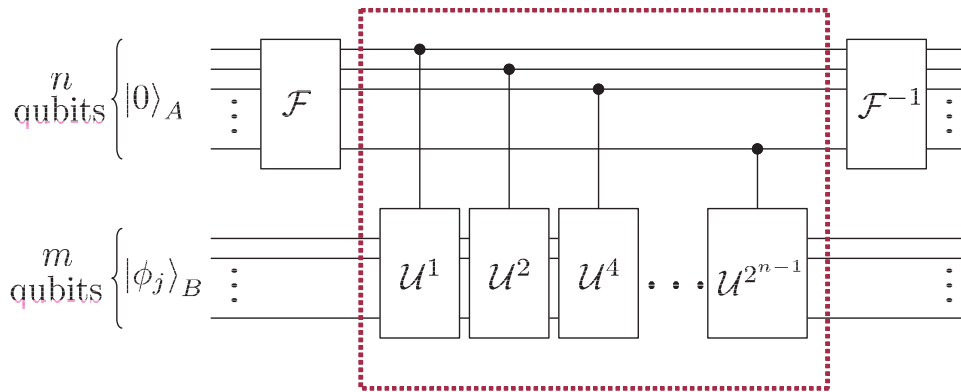


Figure 4: Logic gates for phase-estimation algorithm

state, and so forth.

It is assumed that we can initialize register  $B$  to an eigenstate  $|\phi_j\rangle_B$  of  $\hat{H}$ ; as you will show, the algorithm will yield the leading bits of the eigenvalue  $\lambda_j$  with high probability.

Let's define the gates that are used in the algorithm.  $\mathcal{F}$  is the quantum Fourier transform:

$$|a\rangle_A \xrightarrow{\mathcal{F}} \frac{1}{\sqrt{2^n}} \sum_{b=0}^{2^n-1} e^{i2\pi ab/2^n} |b\rangle_A,$$

and  $\mathcal{F}^{-1}$  is its inverse:

$$|a\rangle_A \xrightarrow{\mathcal{F}^{-1}} \frac{1}{\sqrt{2^n}} \sum_{b=0}^{2^n-1} e^{-i2\pi ab/2^n} |b\rangle_A.$$

The  $\mathcal{U}^x$  gates append phase factors to register  $B$  proportional to the eigenvalue of interest; in this sense, they are analogous to the time evolution operator for the Hamiltonian:

$$|\phi_\ell\rangle \xrightarrow{\mathcal{U}^x} e^{i2\pi x \lambda_\ell} |\phi_\ell\rangle$$

Note that the  $\mathcal{U}^x$  gates are controlled by qubits in register  $A$ ; they are only applied if the control qubits are "1". Assume that  $|\lambda_\ell| \leq 1$ .

- (a) Show that the gates in the dotted box perform the transformation:

$$|a\rangle_A |\phi_j\rangle_B \rightarrow e^{i2\pi a \lambda_j} |a\rangle_A |\phi_j\rangle_B$$

- (b) Calculate the final state of the quantum computer. Show that if  $\lambda_j$  is an integer multiple of  $1/2^n$ , a measurement of register  $A$  in the computational basis gives  $\lambda_j$  in binary form.
- (c) Even if you had a zero-error universal quantum computer of respectable size at your disposal, it is unlikely that this algorithm could be used to examine a problem of interest (perhaps, to find the ground state energy of a collection of a few dozen spins interacting via an antiferromagnetic Heisenberg-model). Why?  
HINT: Initial condition.
- (d) EXTRA CREDIT: Now allow  $\lambda_j$  to take any value between zero and one. Show that a measurement of the  $A$  register gives the leading  $n$  bits of  $\lambda_j$  with probability greater than  $4/\pi^2$ .