QUANTUM INFORMATION AND COMPUTATION
EXERCISE SHEET 4

Nilanjana Datta n.datta@damtp.cam.ac.uk (Lent 2024-2025)

Note: questions 6(b), 7(c) and 8 are optional and can be left till last or omitted.

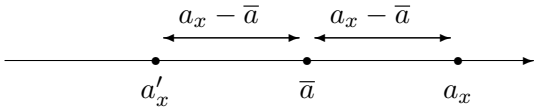
(1) (Rotation in Grover's algorithm)
For the plane $\mathcal{P}(x_0)$ spanned by $|x_0\rangle$ and $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in B_n} |x\rangle$ set up an orthonormal basis in the plane. Then using the basis, show algebraically (rather than geometrically as in lectures) that the Grover iteration operator Q is a rotation in the plane and derive the angle of rotation.

(2) (Grover's algorithm with an arbitrary starting state)
Consider Grover's algorithm for a unique good item x_0 in a search space of size $N = 2^n$. Suppose that instead of the usual uniform superposition state $|\psi_0\rangle$, we start with any state $|\eta_0\rangle$ of n qubits and conduct the algorithm just as before i.e. apply $\frac{\pi}{4}\sqrt{N}$ iterations of Q and measure.
With $|\eta_0\rangle = |\psi_0\rangle$ the final measurement gives x_0 with probability 1 up to terms of order $1/N$. If we instead begin with some other starting state $|\eta_0\rangle$, describe geometrically how $|\eta_0\rangle$ evolves in the course of the computation. Give an expression (up to terms of order $1/N$) for the probability of obtaining x_0 in the final measurement. Show that this may generally be improved by changing the number of Grover iterations.

(3) (An algebraic interpretation of Grover's algorithm)
(a) Consider the operator $-I_{|\psi_0\rangle} = 2\,|\psi_0\rangle\langle\psi_0| - I$ with $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in B_n} |x\rangle$ and $N = 2^n$. Show that

$$-I_{|\psi_0\rangle} = \frac{2}{N} \sum_{\text{all } x,y} |x\rangle\langle y| - I.$$

(b) Let $|\alpha\rangle = \sum_x a_x |x\rangle$ be any n-qubit state. The average amplitude $\overline{a}$ is defined to be $\overline{a} = (\sum_x a_x)/N$. The operation R of "inversion in the average" is defined as follows: $R|\alpha\rangle = \sum_x a'_x |x\rangle$ where $a'_x = a_x - 2(a_x - \overline{a})$ i.e. the value of each amplitude is inverted about the average. Pictorially:



Using the formula in (a) show that $-I_{|\psi_0\rangle}|\alpha\rangle = R|\alpha\rangle$.

(c) Hence Grover's algorithm may be described as follows: start with state $|\psi_0\rangle$; then flip the sign of the x_0 amplitude; then do R, an inversion of all amplitudes in the average; then iterate the last two steps alternately. We can represent states (with real amplitudes) pictorially as a graph of the amplitudes: the x axis has the labels x and each amplitude is a (positive or negative) vertical bar. In terms of this pictorial representation, starting with $|\psi_0\rangle$, carry out one or two iterations of the "flip x_0 and then do R" operation to see how the initial amplitude distribution, uniform over all x, begins to become concentrated at x_0.

(d) Consider the definite case of $N = 4$ (so $x \in \{0, 1, 2, 3\}$) and take $x_0 = 3$ say. (In lectures we saw that for this case of "1 in 4", one Grover iteration serves to find x_0 with certainty i.e. rotating $|\psi_0\rangle$ exactly onto $|x_0\rangle$). Draw the pictorial graph representation of $|\psi_0\rangle$ and carry out one Grover iteration as a flip followed by inversion in the average. Show that as a result, the amplitude becomes exactly zero at $x \neq x_0$ and 1 at $x = x_0$.

(4) (Shor's quantum algorithm for discrete logarithms)
For any prime p consider the set $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\} \subset \mathbb{Z}_p$ of nonzero integers modulo p, with the operation of *multiplication* mod p. A *generator* for $\mathbb{Z}_p^*$ is an element g whose powers generate all of $\mathbb{Z}_p^*$ i.e. for all $x \in \mathbb{Z}_p^*$ there is $y \in \mathbb{Z}_{p-1}$ with $x = g^y \bmod p$. y is called the *discrete logarithm* of x (to base g). You may assume that $\mathbb{Z}_p^*$ always has a generator g and that it satisfies $g^{p-1} = 1 \bmod p$.

Suppose we are given a generator g and element $x \in \mathbb{Z}_p$, and we wish to compute its discrete logarithm y.

(a) Consider the function $f : \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$ given by

$$f(a, b) = g^a x^{-b} \bmod p.$$

For each fixed $c \in \mathbb{Z}_p^*$, show that there is a corresponding fixed $k \in \mathbb{Z}_{p-1}$ such that

$$f(a, b) = c \quad \text{iff} \quad a = by + k \mod (p-1).$$

(b) Suppose we have constructed the state

$$|\phi\rangle = \frac{1}{(p-1)} \sum_{a,b \in \mathbb{Z}_{p-1}} |a\rangle\, |b\rangle\, |f(a, b)\rangle$$

(in $\mathcal{H}_{p-1} \otimes \mathcal{H}_{p-1} \otimes \mathcal{H}_p$, where $\mathcal{H}_n$ denotes a state space of dimension n, with orthonormal basis $\{|k\rangle : k \in \mathbb{Z}_n\}$) and we measure the third register obtaining a result c_0. Find the post-measurement state of the first two registers.

(c) If we then apply the quantum Fourier transform mod $(p-1)$ to each of these two registers and measure both registers, which output pairs $(c_1, c_2) \in \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$ can be obtained with non-zero probability?
Can y be determined from any such pair?
Hence outline a quantum algorithm for computing discrete logarithms, that runs in time $O(\text{poly}(\log p))$ for large p, and succeeds with probability $1 - \epsilon$ for any chosen constant $\epsilon > 0$. You may assume that f and QFT_{p-1} may be implemented in $O(\text{poly}(\log p))$ time.

(5) (Shor's factoring algorithm, continued fractions)
This question relates closely to §11.1 - §11.3 of online lecture notes.
Suppose we wish to factor $N = 21$ using Shor's algorithm and we have chosen $a = 2$ so we aim to determine the period of $f(x) = 2^x \bmod 21$. We proceed through the quantum algorithm and finally measure the x register. Suppose we obtain measurement result $c = 427$.

(a) What is the number m of qubits that is used for the x register?

(b) Use the continued fraction method to find a fraction j/r with denominator less than 21, that is within $1/2^{m+1}$ of the ratio $c/2^m$.

(c) We hope that the denominator of j/r (when the fraction is cancelled down to lowest terms) is the period of $f(x)$. Check to see that it is indeed the period in this example.
Use your value of r to find factors of 21 (following the method used in Shor's algorithm).

(6) (Grover search with multiple good items; application to collision finding)
(a) Write $N = 2^n$ and let $f : B_n \to B_1$ be a function taking value 1 exactly K times, with $f(x) = 1$ iff $x \in G = \{x_1, \ldots, x_K\}$. The Grover operator is defined by $Q = -H_n I_0 H_n I_G$ where $H_n = H \otimes \ldots \otimes H$ is the Hadamard operation on each of n qubits, and for all $x \in \mathcal{B}_n$, I_0 and I_G are defined by

$$I_0 |x\rangle = \begin{cases} -|x\rangle & \text{if } x = 0 \ldots 0 \\ |x\rangle & \text{if } x \neq 0 \ldots 0 \end{cases} \qquad I_G |x\rangle = \begin{cases} -|x\rangle & \text{if } x \in G \\ |x\rangle & \text{if } x \notin G. \end{cases}$$

Write $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in B_n} |x\rangle$ and introduce $|\psi_G\rangle = \frac{1}{\sqrt{K}} \sum_{x \in G} |x\rangle$. Derive a geometrical interpretation of the action of Q in the two-dimensional subspace of n qubits spanned by $|\psi_0\rangle$ and $|\psi_G\rangle$. Using this interpretation, show that if I_G is given as a black box then an x in G may be obtained with high probability (better than a half say) with $O(\sqrt{N/K})$ uses of I_G, if N is large, and K is small compared to N.

(b) (optional) Let $g : B_n \to B_n$ be a 2-to-1 function i.e. for every y in the range of g there are precisely two strings $x \in B_n$ with $g(x) = y$. A *collision* is a pair of strings $x_1, x_2 \in B_n$ with $g(x_1) = g(x_2)$. The standard quantum oracle U_g for g is the unitary operation on $2n$ qubits defined by

$$U_g |x\rangle |y\rangle = |x\rangle |y \oplus g(x)\rangle \qquad x, y \in B_n$$

where $\oplus$ denotes bitwise addition of n-bit strings.

Suppose that we are given U_g as a black box operation. Using the result of (a), or otherwise, show that a collision may be found with high probability (better than a half say) with $O(N^{1/3})$ uses of U_g.
Hint: start by partitioning the domain of g into sets A and B of sizes $N^{1/3}$ and $(N - N^{1/3})$ and listing all the values of $g(x)$ for $x \in A$. We might find a collision there, but if we're not so lucky, what should we do next with B?

Remark: the classical query complexity for collision finding is $O(\sqrt{N})$. The $O(N^{1/3})$ upper bound on its quantum query complexity established in this question can also be shown to be optimal.

(7) (QFT, shift invariant states)
(a) For the state space $\mathcal{H}_N$ with orthonormal basis $\{|k\rangle : k \in \mathbb{Z}_N\}$ consider the (unitary) shift operator S defined by $S|k\rangle = |k + 1 \bmod N\rangle$ for all $k \in \mathbb{Z}_N$. Also introduce the states $|\chi_k\rangle = QFT_N |k\rangle$, called *shift invariant states.*

Show that the $|\chi_k\rangle$'s are eigenstates of S and determine the corresponding eigenvalues.

Let $|\psi\rangle$ be any state in $\mathcal{H}_N$. Show (using the foregoing) that if $S^m |\psi\rangle$ (for any m) is measured relative to the shift invariant basis then the output probabilities are independent of the amount of shift m. (This provides an alternative derivation of the efficacy of QFT in the quantum period finding algorithm, as presented in lectures).

(b) For any two positive integers x and N with $x < N$, and let U_x be the operator on $\mathcal{H}_N$ defined by $U_x |y\rangle = |xy \bmod N\rangle$ for all $y \in \mathbb{Z}_N$ i.e. U_x is the shift operator for the *multiplicative* (rather than additive) action of x on $\mathbb{Z}_N$.

(i) Show that U_x is unitary iff x and N are coprime.

Assume now that x and N are coprime. Let r be the order of x mod N (i.e. the minimal $t > 0$ such that $x^t = 1 \bmod N$). For $0 \leq s \leq r - 1$, define the states

$$|\psi_s\rangle := \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k / r} \left| x^k \bmod N \right\rangle .$$

(ii) Show that each state $|\psi_s\rangle$ is an eigenvector of U_x with eigenvalue $e^{2\pi is/r}$ (i.e. these are shift invariant states for the multiplicative action).

(iii) Show that $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\psi_s\rangle = |1\rangle$.

(c) (Optional) Suppose now that we have a quantum process $\mathcal{A}$ that achieves the following: for any unitary V, if $|\xi_\lambda\rangle$ is any eigenstate of V with eigenvalue $e^{2\pi i\lambda}$ then $\mathcal{A}$ is a unitary process which on input $|\xi_\lambda\rangle |0\rangle$ produces the final state $|\xi_\lambda\rangle |\lambda\rangle$ (from which the value of λ may be read out by a measurement on the second register). Here the second register (initially $|0\rangle$) is of suitable size to be able to represent the possible values of λ (and we are ignoring issues of precision here). Such a process $\mathcal{A}$ does in fact exist and is usually called the *phase estimation algorithm*. For the purposes of this question we will assume that $\mathcal{A}$ is given for the case of $V = U_x$, and also that in this case, it runs in poly($\log N$)-time (which is true). (For an account of the phase estimation algorithm see e.g. Nielsen and Chuang §5.2).

Show how the results of (b) together with the phase estimation algorithm for $V = U_x$ can be used to provide a poly($\log N$)-time quantum algorithm for factoring N (called Kitaev's factoring algorithm). Hint: start with the reduction of factoring to order finding, as done in Shor's algorithm.

(8) (A query complexity problem with no promise) (optional)
Let $\mathbf{x} = x_0 x_1 \dots x_{N-1}$ be an N-bit string. We may think of $\mathbf{x}$ as the list of values of a function from $\mathbb{Z}_N$ to $\{0,1\}$. A quantum oracle $O_\mathbf{x}$ for $\mathbf{x}$ is a unitary operation on a state space of dimension $2N$ whose action is defined by $O_\mathbf{x} |i\rangle |y\rangle = |i\rangle |y \oplus x_i\rangle$, where $i \in \mathbb{Z}_N$, $y \in \{0,1\}$ and $\oplus$ denotes addition modulo 2.
Note: this simply generalises the notion of an oracle for $f : B_n \to B_1$ (corresponding to domain size $N = 2^n$) to arbitrary sized domains that are not powers of 2.

Consider the following oracle problem BAL:
Input: an oracle $O_\mathbf{x}$ for some N-bit string $\mathbf{x}$ with $N = 2K$ being even.
Problem: decide *with certainty* whether $\mathbf{x}$ is (i) balanced or (ii) not balanced. (Here 'balanced' means that exactly half of the bit values are 0 and half are 1).

We know that if we impose a promise on $\mathbf{x}$ that it is either balanced or constant, then the problem can be solved with just one query to the oracle (by the Deutsch-Jozsa algorithm). But if there is no promise on the form of $\mathbf{x}$ (as in BAL) then it can be shown that any quantum algorithm solving it requires at least $O(N^{\frac{1}{6}})$ queries to the oracle (so is exponential in n for $N = 2^n$). The actual (optimal) quantum query complexity is not known.

(a) Show that any classical deterministic algorithm that solves Problem BAL on any input must make at least $N = 2K$ queries to the oracle in the worst case.

We now develop a quantum algorithm that solves BAL with at most $K = N/2$ queries thus improving (albeit modestly) on any classical algorithm.

(b) Begin by writing $\hat{x}_i = (-1)^{x_i}$ and we will work on a state space of dimension N^2 with orthonormal basis states $|i\rangle |j\rangle$ for $i, j \in \mathbb{Z}_N$. Consider the following three computational steps:

Step 1: Make the state $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle |0\rangle$ and then (together with a qubit in state $|-\rangle$) use one query to the oracle to make

$$|\psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \hat{x}_i |i\rangle |0\rangle .$$

Step 2: Consider a transformation U whose action on states $|i\rangle\,|0\rangle$ is given by

$$U : |i\rangle\,|0\rangle \to \frac{1}{\sqrt{N}}\left(\sum_{k>i}|i\rangle\,|k\rangle - \sum_{k<i}|k\rangle\,|i\rangle + |0\rangle\,|0\rangle\right).$$

Then by linearity the action of U on $|\psi_1\rangle$ will be

$$|\psi_2\rangle = U\,|\psi_1\rangle = \left(\frac{1}{N}\sum_{i=0}^{N-1}\hat{x}_i\right)|0\rangle\,|0\rangle + \sum_{i<j}\frac{(\hat{x}_i - \hat{x}_j)}{N}\,|i\rangle\,|j\rangle$$

as you can directly check.

Step 3: Measure $|\psi_2\rangle$ to obtain an outcome (k, l) with $k, l \in \mathbb{Z}_N$.

(i) Show that there exists a *unitary* transformation $\tilde{U}$ on the whole state space whose action on the states $|i\rangle\,|0\rangle$ coincides with the action of U as given in step 2.

(ii) Suppose for a moment that we impose the promise on $\mathbf{x}$ that it is either balanced or constant. If we see $(0, 0)$, respectively $(i, j) \neq (0, 0)$, as the measurement outcome in step 3, what can we deduce about the string $\mathbf{x}$?

(iii) Now returning to general input strings $\mathbf{x}$ and considering the possible measurement outcomes (k, l), show that Problem BAL may be solved with certainty with at most $K = N/2$ queries to the oracle in every case (by suitable uses of the steps above).