QUANTUM INFORMATION AND COMPUTATION
EXERCISE SHEET 4

Nilanjana Datta n.datta@damtp.cam.ac.uk (Lent 2025-2026)

(1) (Another query complexity problem with quantum advantage)
Let B_n denote the set of all n-bit strings. The Hamming distance between two n-bit strings $a = a_1 \dots a_n$ and $x = x_1 \dots x_n$ is the number of places j where a_j and x_j differ. Let $H_a : B_n \to B_2$ be the function

$$H_a(x) = (\text{Hamming distance between } a \text{ and } x) \bmod 4.$$

Here we are identifying B_2 with $\mathbb{Z}_4$ via the usual binary representations of 0,1,2,3. (For example if $a = 101110000$ and $x = 001001110$ then $H_a(x) = 6 \bmod 4 = 2$.)

Now consider the promise problem **HAM-mod4**:
Input: a black box for a function $f : B_n \to B_2$.
Promise: f is H_a for some n-bit string a.
Problem: determine a with certainty.

In the quantum context the black box is a unitary operation on $(n+2)$ qubits given by

$$U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y + f(x)\right\rangle .$$

Here the x register is n qubits and in the y register we'll write the basis as $\{\left|0\right\rangle, \left|1\right\rangle, \left|2\right\rangle, \left|3\right\rangle\}$ with addition in the expression $y + f(x)$ being addition in $\mathbb{Z}_4$.

(a) Show that classically the query complexity of **HAM-mod4** is at least $n/2$.

We will now show that the problem can be solved quantumly with just *one* query. Let M be the matrix

$$M = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}.$$

Note that M is unitary. Also introduce the 1-bit functions $h_0, h_1 : B_1 \to B_1$ where

$$h_0(0) = 0 \;\; h_0(1) = 1 \quad \text{and} \quad h_1(0) = 1 \;\; h_1(1) = 0$$

i.e. h_a is just H_a for 1-bit string a.

(b) For $a_1 = 0, 1$ show that

$$M \left|a_1\right\rangle = \frac{1}{\sqrt{2}} \sum_{x_1=0}^{1} i^{h_{a_1}(x_1)} \left|x_1\right\rangle .$$

(c) Returning to the case of n-bit strings $a = a_1 \dots a_n$ and $x = x_1 \dots x_n$ show that

$$H_a(x) = h_{a_1}(x_1) + \dots + h_{a_n}(x_n) \bmod 4.$$

Hence describe how the state

$$\left|H_a\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in B_n} i^{H_a(x)} \left|x\right\rangle$$

may be manufactured from $\left|a\right\rangle$.

(d) Let S denote the 2-qubit "shift" operation

$$S \left|y\right\rangle = \left|y + 1 \bmod 4\right\rangle \quad y \in \mathbb{Z}_4.$$

Let QFT denote the quantum Fourier transform mod 4. Calculate the state $|\psi_3\rangle = QFT\,|3\rangle$ and show that $S\,|\psi_3\rangle = i\,|\psi_3\rangle$.

(e) Use the above results to show how **HAM-mod4** may be solved with certainty using just one query to the oracle U_f and poly(n) total time complexity. (It may be helpful to note that $U_{H_a}\,|x\rangle\,|y\rangle = |x\rangle\,S^{H_a(x)}\,|y\rangle$.)
Draw a circuit diagram for your quantum algorithm.

[Optional afterthought: note that this algorithm is structurally "the same as" the Bernstein-Vazirani (BV) algorithm and it is interesting to compare the corresponding ingredients and their functionality. What are the BV ingredients corresponding to the use of QFT, $|\psi_3\rangle$, M, h_a and H_a here?]

(2) (Period finding algorithm)
Consider the function $f(x) = 5^x \bmod 39$ on the domain $x \in \mathbb{Z}_{2^m}$ with say $m = 11$ (as in fact would occur in Shor's algorithm for factoring 39).

(a) Show that f is periodic and determine its period r (hmm.. reach for a calculator.)

(b) Suppose we construct the equal superposition state $|f\rangle$ of $(x, f(x))$ values over the domain $\mathbb{Z}_{2^m}$, measure the second register, perform the quantum Fourier transform mod 2^m on the post-measurement state of the first register, and finally measure it. What is the probability for each possible outcome $0 \le c < 2^m$ in the latter measurement? (Note: this should require very little calculation!) What is the probability that we successfully determine r from this measurement result, using the standard process of the quantum period finding algorithm?

(3) (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.

(4) (Shor's factoring algorithm, continued fractions)
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).

(5) (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 $x \bmod N$ (i.e. the minimal $t > 0$ such that $x^t = 1 \bmod N$). For $0 \le s \le r-1$, 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 $e^{2\pi i s/r}$ (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.

(6) (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).

(7) (Approximately universal quantum gate sets)
(a) For unitary gates U_1, V_1, U_2, V_2 show that:
if $||U_1 - V_1|| \leq \epsilon_1$ and $||U_2 - V_2|| \leq \epsilon_2$ (i.e. the V's are "approximate versions" of the U's)
then $||U_2 U_1 - V_2 V_1|| \leq \epsilon_1 + \epsilon_2$ i.e. "errors" in using approximate versions at most add when gates are composed.
(Recall that here $||U - V||$ is defined as the maximum length of the vector $(U - V)|\psi\rangle$ over all choices of normalised $|\psi\rangle$'s.)

Deduce that if $||U_i - V_i|| \leq \epsilon$ for $i = 1, \ldots, n$ then $||U_n \ldots U_1 - V_n \ldots V_1|| \leq n\epsilon$.

(b) For the purposes of this question you may assume the following: if a gate set $\mathcal{S}$ is approximately universal then any one- or two-qubit gate U may be approximated to within ϵ by a circuit of gates from $\mathcal{S}$ of size $\text{poly}(1/\epsilon)$. (Actually by the Solovay-Kitaev theorem, mentioned in lectures, a stronger result is true viz. that a circuit of much smaller size $\text{poly}(\log(1/\epsilon))$ suffices, but we will not need that improvement here.)

Let $\mathcal{G}$ and $\mathcal{H}$ be two approximately universal sets of gates comprising one- and two-qubit gates only. Suppose that the decision problem D is in the complexity class **BQP** with all quantum gates in the circuits being from the set $\mathcal{G}$. Show that D is then also in the class **BQP** defined using quantum gates from the set $\mathcal{H}$ i.e. the definition of **BQP** is independent of the choice of approximately universal set of gates used.

(8) (Entanglement is necessary for advantage in quantum computation)
Consider a quantum computation, given as a poly-sized circuit family $\{C_1, C_2, \ldots, C_n, \ldots\}$ where each C_n comprises gates from a universal set $\mathcal{G}$ comprising one- and two-qubit gates, and suppose that this computation solves a decision problem A in **BQP**.
Suppose further that for any input $x \in B_n$ to the circuit C_n (for any n), at every stage of the process, the quantum state is *unentangled* i.e. it is a product state of all the qubits involved.
Show that then the problem A is also in **BPP** i.e. if no entanglement is ever present in a quantum computation, then it cannot provide any computational benefit over classical computation (up to at most a polynomial overhead in time). (Hint: consider calculating the progress of the quantum process itself on a classical computer).