Part III QUANTUM COMPUTATION
EXERCISE SHEET 2

Richard Jozsa rj310@cam.ac.uk (November 2020)

(1) (Making Grover search and Ampl Ampl exact)
Grover search (and more generally the amplitude amplification process) does not usually return a good item with *certainty* but only with some high probability (why?). However Grover search (and AA) can be modified to work with probability 1, as follows.

(a) Suppose we have the n-qubit starting state for the AA process:

$$|\psi\rangle = \alpha\,|g\rangle + \beta\,|b\rangle$$

where as usual, α and β are real and positive, and $|g\rangle$ and $|b\rangle$ are the good and bad projections of $|\psi\rangle$ re-normalised to unit length. Suppose that the good and bad subspaces are spanned by computational basis states and the indicator function $f(x) = 0$ resp. 1 for x good resp. bad, can be computed, and that $|\psi\rangle = W\,|0\ldots0\rangle$ for an implementable n-qubit unitary W. *Suppose also that the value of α is known.*
By adjoining an extra qubit (and suitably extending the notion of goodness/badness from x to $x0$ and $x1$), show that the AA process above can be modified (by a suitable extension) to become exact i.e. the final measurement of the modified process will yield a good x with certainty. [Hint: for one possible approach recall Grover search for "1 in 4".]

(b) Suppose we are given two distinct primes p and q and the product $N = pq$ has n digits when written in binary i.e. $2^n/2 \leq N < 2^n$. Consider the quantum state

$$|\xi\rangle = \frac{1}{\sqrt{|A|}} \sum_{k\in A} |k\rangle$$

where $A = \{k : 1 \leq k \leq N \text{ and } k \text{ is coprime to } N\}$, and $|A|$ denotes the size of the set A. Here all integers are written in binary as n-bit strings (adjoining leading higher order bits set to zero if needed) so $|\xi\rangle$ is an n-qubit state.
(i) Show that $|A| = (p-1)(q-1)$.
(ii) Describe how the state $|\xi\rangle$ may be prepared with certainty in an n-qubit register, starting with each qubit initially in state $|0\rangle$.
Can your preparation process be implemented in poly(n) time?

(2) (Kitaev's algorithm for order finding and factoring, using phase estimation)
Fix two coprime positive integers x and N such that $x < N$. On a state space with basis $\{|y\rangle : y = 1, 2, \ldots, N\}$ let U_x be the operator defined by $U_x\,|y\rangle = |xy \bmod N\rangle$. Let r be the order of x mod N (the minimal t such that $x^t \equiv 1 \bmod N$). For $0 \leq s \leq r-1$, introduce the states

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

(a) Verify that U_x is unitary. Show that the states $|\psi_s\rangle$ are all eigenvectors of U_x and determine the corresponding eigenvalues.

(b) Show that $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\psi_s\rangle = |1\rangle$. Describe how, for any n, the phase estimation algorithm may be used to provide (with constant probability) an estimate of s/r accurate to n bits, where $0 \leq s < r$ has been chosen uniformly at random.

(c) Let N have m binary digits (i.e. $2^{m-1} < N < 2^m$). Show that if a $(2m+1)$-bit approximation ξ to s/r is given then the exact value of s/r is uniquely determined. (How close to each other

can any two different fractions of the form s/r with $r < N$ be?) You may assume that the exact value may be determined from ξ *efficiently* i.e. in time poly$(\log N)$. (In fact this may be achieved by using the theory of continued fractions cf. Part II notes for an account of how it works).

(d) It can be shown that the operation $U_x^{2^k}$ may be implemented efficiently in k i.e. in time poly(k). This can be shown from the fact that the classical computation of $x \to x^{2^k} \bmod N$ can be efficiently computed by k iterated squarings ($z \to z^2$, starting with $z = x$) in contrast to the exponentially slower multiplication of x by itself 2^k times.
Assuming the foregoing fact, show how the above ingredients can be used to provide an efficient (i.e. poly$(\log N)$ time) quantum algorithm that computes the order of x mod N and succeeds with any desired probability $1 - \epsilon < 1$. Then using the same classical reduction of order finding to factoring that was used in Shor's algorithm, note that this also provides an efficient quantum algorithm for factoring.

(3) (A nested Grover search)
Consider the *unique collision problem* UCP:
Input: an oracle for $f : B_n \to B_n$;
Promise: f is one-to-one on all inputs except for a single pair x_1, x_2 with $f(x_1) = f(x_2)$ i.e. f has a unique "collision";
Problem: determine x_1 and x_2.
Let Q be the query complexity of UCP and write $N = 2^n$.

(a) Show that $O(N)$ is an upper bound for Q. Show that $O(\sqrt{N})$ is a lower bound. [Hint: display a reduction from unique Grover search to UCP.]
Thus $O(\sqrt{N}) < Q < O(N)$. We'll now develop an algorithm for UCP that uses $O(N^{3/4})$ queries.
Remark: using different methods (quantum walk algorithms, not treated in this course) it can be shown that the optimal number of queries necessary and sufficient to solve UCP is $O(N^{2/3})$ cf. A. Ambainis arXix:quant-ph/0311001.

(b) Divide the domain B_n into subsets A_k each of size $\sqrt{N}$. Define k to be "good" if A_k contains *both* of x_1 and x_2. Describe an algorithm that will find a good k if it exists (and in that case it also finds x_1 and x_2) and the algorithm makes $O(N^{3/4})$ queries to f. [Hint: note that any k may be tested for goodness using $\sqrt{N}$ queries.]

(c) Alas, it is quite likely that x_1 and x_2 will be in different A_k's so the algorithm in (b) will fail to find a good k. In that case, continue as follows: we now define k to be "good" if A_k contains *one* of x_1 and x_2 (so the other of these must be in $\overline{A}_k = B_n - A_k$). Introduce the indicator function $g(k)$ which is 1 if k is good, and 0 if k is bad. Describe an algorithm that computes $g(k)$ for any given k, using $O(\sqrt{N})$ queries to f. [Hint: consider a suitable Grover search!]

(d) By considering a further Grover search (that suitably incorporates the algorithm of (c)) show that UCP can be solved with $O(N^{3/4})$ queries.

(4) (Grover search with an unknown number of good items)
(a) Consider the unit circle with equally spaced points at (small) angle γ apart (except possibly for one angle $< \gamma$ to complete the circle). Show that if l is any line through the centre then at least a fraction $\frac{1}{2} - \frac{2\gamma}{\pi}$ of the points must lie within $\pm 45^\circ$ of l.

(b) Consider Grover search with function $f : B_n \to B_1$ having k good x's but k being unknown. Write $N = 2^n$. Assume also that $k << N$ so arcsin $\sqrt{k/N}$ can be well approximated as $\sqrt{k/N}$. The standard Grover search algorithm cannot then be applied (why?). By choosing the number K of iterations of the Grover operator in the standard algorithm uniformly at random in the range $0 < K < \pi\sqrt{N}$, show how a good x may be found with probability at least c for a

constant $c > 0$. Deduce that a good x may be found with any desired probability of success $1 - \epsilon$ ($\epsilon > 0$) using $O(\sqrt{N})$ queries to f.

(5) (Implementing reflection operators) (optional)
In Grover search (with $f : B_n \to B_1$ and k 'good' x's in B_n) it is important that the n-qubit reflection operators $I_{|\psi_0\rangle}$ (with $|\psi_0\rangle$ being the usual uniform superposition of all $|x\rangle$'s) and I_G are not prohibitively expensive to implement e.g. not requiring say exponential sized circuits.

(a) Show that I_G can be implemented in poly(n) time if f can be implemented in poly(n) time.

(b) For the reflection $I_{|\psi_0\rangle}$ we'll develop an explicit $O(n)$ sized circuit of constant sized gates (each acting on at most 3 qubits).
Consider the 3-qubit Toffoli gate (or doubly-controlled NOT gate) defined by

$$T_{123} |a\rangle_1 |b\rangle_2 |c\rangle_3 = \begin{cases} |a\rangle_1 |b\rangle_2 X |c\rangle_3 & \text{if } a = b = 1 \\ |a\rangle_1 |b\rangle_2 |c\rangle_3 & \text{otherwise} \end{cases} \qquad \text{for all } a, b, c \in B_1.$$

Note (i.e. show) that T is the usual quantum oracle U_g for $g : B_2 \to B_1$ with $g(a, b) = ab$.

(i) Consider $2n$ qubit registers comprising n registers labelled $1, 2, \ldots, n$ together with $n-1$ 'work space' registers labelled $w_1, \ldots, w_{n-1}$ and a target qubit labelled t. Show how the transformation

$$|c_1\rangle_1 \ldots |c_n\rangle_n |0\rangle_{w_1} \ldots |0\rangle_{w_{n-1}} |y\rangle_t \longrightarrow |c_1\rangle_1 \ldots |c_n\rangle_n |0\rangle_{w_1} \ldots |0\rangle_{w_{n-1}} |y \oplus c_1 c_2 \ldots c_n\rangle_t$$

for any $c_1, \ldots, c_n, y \in B_1$, may be implemented using $(2n - 2)$ Toffoli gates and one CX gate. Hint: it may help to consider first the action of T_{12w_1} followed by $T_{3w_1w_2}$, and for simplicity take say $n = 4$.

(ii) Deduce that $I_{|00\ldots0\rangle}$ and $I_{|\psi_0\rangle}$ can be implemented with $O(n)$ sized circuits of gates each acting on at most 3 qubits (also with availability of $O(n)$ sized work space).

(6) (More efficient quantum simulation)
(a) Let A and B be Hermitian operators with $\|A\| \leq K$, $\|B\| \leq K$ for some $K \leq 1$. Show that

$$e^{-iA/2} e^{-iB} e^{-iA/2} = e^{-i(A+B)} + O(K^3)$$

(this is the so-called *Strang splitting*). Use this to give a more efficient approximation of k-local Hamiltonians by quantum circuits than the algorithm given in the notes, and calculate its complexity.

(b) Let H be a Hamiltonian which can be written as $H = UDU^\dagger$, where U is a unitary matrix that can be implemented by a poly(n)-sized quantum circuit, and $D = \sum_x d(x) |x\rangle \langle x|$ is a diagonal matrix such that $|x\rangle \mapsto e^{-id(x)t} |x\rangle$ can be implemented in poly(n)-time. Show that then e^{-iHt} can be implemented in poly(n)-time.