QUANTUM COMPUTATION – EXERCISE SHEET 1

Richard Jozsa rj310@cam.ac.uk (October 2016)

(1) Let $|\psi\rangle$ be any state of n qubits and let $1 \leq A \neq B \leq n$. Using the extended Born rule show that the output distribution of a measurement of qubit A is unaffected by whether or not qubit B is measured prior to the measurement of A.
Remark: this is part of the *no-signalling principle* in quantum mechanics viz. suppose that A ad B are distantly separated in space. Then although a measurement of B immediately before that of A instantaneously changes the state description at A (into a probabilistic mixture of the post-measurement states of B's measurement), A cannot notice this change by any local measurement statistics (or indeed in any other way).

(2) (Principle of deferred measurements)
(a) Consider the quantum controlled operation W on m qubits (with qubit 1 as the control) given by the following descriptrion:
if qubit 1 is $|0\rangle$ apply U to qubits $2, \ldots, m$;
if qubit 1 is $|1\rangle$ apply V to qubits $2, \ldots, m$.
Show how W may be implemented using only gates from the set U, V, controlled$-U$, controlled$-V$ and their inverses.
(b) The *principle of deferred measurements* states:
Any circuit with intermediate measurements can always be replaced by an equivalent circuit having only unitary gates and all measurements only at the end of the circuit; if the intermediate measurement results are used at any stage in the original circuit for choice of later gates, then these classically controlled operations can be replaced by quantum controlled operations (or the kind in (a)). To see why this is true consider the following illustrative example of two computational processes on three qubits initially in state $|0\rangle_1 |0\rangle_2 |0\rangle_3$:
(COMP1): apply unitary gate A to the three qubits to obtain $|\alpha\rangle = A|0\rangle_1 |0\rangle_2 |0\rangle_3$. Then measure qubit 1. If the result is 0 (resp. 1) then apply unitary U (resp. V) to qubits 2 and 3. Finally measure qubit 2 to obtain the output.
(COMP2): apply unitary gate A to the three qubits to obtain $|\alpha\rangle = A|0\rangle_1 |0\rangle_2 |0\rangle_3$. Introduce an extra 'ancilla' qubit $|0\rangle_0$ and apply CX_{10} (so qubit 1 is the control and the ancilla is the target). Apply the controlled quantum operation W of (a) (with $m = 3$ there) to qubits 1,2,3. Finally measure qubit 2 to obtain the output.
Show that the output distributions of (COMP1) and (COMP2) are identical.
Remarks: Note that the intermediate measurement and classically controlled further gates in (COMP1) have been replaced in (COMP2) by a fully unitary circuit. In the same way, any intermediate measurements in any quantum circuit can be simulated by a circuit of only unitary gates (with no intermediate measurements) at the expense of introducing a further ancillary qubit for each intermediate measurement, and use of appropriate quantum controlled operations.
In view of question 1, we could have measured qubit 0 at the end too without affecting the output distribution at qubit 2 i.e. instead of eliminating the intermediate measurement altogether we can think of this as moving it to the end.

(3) (Bernstein-Vazirani problem)
For n-bit strings $x = x_1 \ldots x_n$ and $a = a_1 \ldots a_n$ in B_n we have the sum $x \oplus a$ which is an n-bit string, and now introduce the 1-bit "dot product" $x \cdot a = x_1 a_1 \oplus x_2 a_2 \oplus \ldots \oplus x_n a_n$.
For any fixed n-bit string $a = a_1 \ldots a_n$ with $a \neq 00 \ldots 0$, consider the function $f_a : B_n \to B_1$ given by

$$f_a(x_1, \ldots, x_n) = x \cdot a \tag{1}$$

(a) Show that for any $a \neq 00 \ldots 0$, f_a is a balanced function i.e. f_a has value 0 (respectively 1)

on exactly half of its inputs x.
(b) Given a classical black box that computes f_a describe a classical deterministic algorithm that will identify the string $a = a_1 \dots a_n$ on which f_a is based. Show that *any* such black box classical algorithm must have query complexity at least n.

Now for any n let $H_n = H \otimes \dots \otimes H$ be the application of H to each qubit of a row of n qubits. Show that (for $x \in B_1$ and $a \in B_n$)

$$H|x\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{xy} |y\rangle \qquad H_n|a\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in B_n} (-1)^{a \cdot y} |y\rangle$$

(c) (the Bernstein–Vazirani problem)
For each a consider the function f_a which is a balanced function if $a \neq 00\dots0$ (as shown above). Show that the DJ algorithm will perfectly distinguish and identify the $2^n - 1$ balanced functions f_a (for $a \neq 00\dots0$) with only *one* query to the function – in fact show that the n bit output of the algorithm gives the string a with certainty for these special balanced functions.

(4) (Classical complexity – integer exponentiation mod N)
In Shor's algorithm we need to compute the exponentiation of integers mod N and it is important to know that this can be done efficiently. To compute say $3^k \bmod N$ (for $0 \leq k \leq N-1$) we could multiply 3 together k times. Show that this is not a polynomial time computation (i.e. not poly time in $n = \log N$, the largest possible input size for k).
Devise an algorithm that *does* run in poly(n) time. (Hint: consider repeated squaring).
You may assume that multiplication mod N of a pair of integers with n digits may be done in $O(n^2)$ time.
Generalise to a poly time computation of $k_1^{k_2} \bmod N$ for $0 \leq k_1, k_2 \leq N-1$ showing that it may be computed in $O(n^3)$ time.

(5) (Simon's algorithm)
Simon's decision problem is the following:
Input: an oracle for a function $f : B_n \to B_n$,
Promise: f is either (a) a one-to-one function or (b) a two-to-one function of the following special form – there is an $\xi \in B_n$ such that $f(x) = f(y)$ iff $y = x \oplus \xi$ (i.e. ξ is the period of f when its domain is viewed as being the group $(\mathbb{Z}_2)^n$).
Problem: determine which of (a) or (b) applies (with bounded error probability $1 - \epsilon$ for any $\epsilon > 0$).

It can be argued (cf lecture notes) that the classical randomised query complexity of this problem is $O(2^{n/4})$. In this question we will develop a quantum algorithm that that solves the problem with quantum query complexity only $O(n)$. Even more, the algorithm will determine the period ξ if (b) holds. Thus (unlike the balanced vs. constant problem) we'll have a provable exponential separation between classical and quantum query complexities, even in the presence of bounded error.

To begin, consider $2n$ qubits with the first (resp. last) n comprising the input (resp. output) register for a quantum oracle U_f computing f i.e. $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ for n-bit strings x and y.
(a) With all qubits starting in state $|0\rangle$ apply H to each qubit of the input register, query U_f and then measure the output register. Write down the generic form of the n-qubit state $|\alpha\rangle$ of the input register, obtained after the measurement. Suppose we were to measure $|\alpha\rangle$. Would the result provide any information about the period ξ?
(b) Having obtained $|\alpha\rangle$ as in (a), apply H to each qubit to obtain a state denoted $|\beta\rangle$. Show that if we measure $|\beta\rangle$ then the n-bit outcome is a uniformly random n-bit string y satisfying $\xi \cdot y = 0$ (so any such y is obtained with probability $1/2^{n-1}$).

Now we can run this algorithm repeatedly, each time independently obtaining another string y satisfying $\xi \cdot y = 0$. Recall that $B_n = (\mathbb{Z}_2)^n$ is a vector space over the field $\mathbb{Z}_2$. If $y_1, \ldots, y_s$ are s linearly independent vectors (bitstrings) then their span contains 2^s of the 2^n vectors in B_n. Furthermore to solve systems of linear equations over B_n we can use, for example, the standard Gaussian elimination method (calculating with the algebra of the field $\mathbb{Z}_2$).

(c)* Show that if $(n-1)$ bitstrings y are chosen uniformly randomly and independently satisfying $y \cdot \xi = 0$ then they will be linearly independent with probability at least $1/4$.
(d) Let $0 < p < 1$ be any chosen constant probability. Show that $K = O(n)$ runs of the algorithm in (a) and (b) will suffice to determine ξ with probability at least p. Writing $K = kn$ give an expression for k as a function of p.
(e) The above gives a bounded error algorithm for finding the period ξ assuming that the given function was in fact periodic. Show how this may be used to solve Simon's problem with $O(n)$ query complexity (and with bounded error).

(6) (Entanglement necessary in quantum computation)
Consider a quantum computation, given as a polynomial-sized circuit family $\{C_1, C_2, \ldots, C_n, \ldots\}$ where each C_n comprises gates from the universal set $\{H, S, CX\}$ (where S denotes the $\pi/8$ phase gate) and suppose that this computation solves a decision problem $\mathcal{A}$ in **BQP**.
Suppose further that for any input $x \in B_n$ to 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 $\mathcal{A}$ 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 a poly overhead in time).

(7) (Making 2-qubit states)
(a) Let $\{|\alpha_0\rangle, |\alpha_1\rangle\}$ be any orthonormal basis for a qubit. Show that there is a 1-qubit unitary gate U with $U|0\rangle = |\alpha_0\rangle$ and $U|1\rangle = |\alpha_1\rangle$.

(b) Let $|\psi\rangle$ be any 2-qubit state. Is it possible to manufacture $|\psi\rangle$ from $|0\rangle|0\rangle$ by the application of a circuit comprising only 1-qubit gates (which are otherwise unrestricted)? Give a reason for your answer.

(c) The Schmidt decomposition theorem for 2-qubit states is the following:
Theorem: if $|\psi\rangle$ is any 2-qubit state then there are orthonormal bases $\{|\alpha_0\rangle, |\alpha_1\rangle\}$ and $\{|\beta_0\rangle, |\beta_1\rangle\}$ and non-negative real numbers λ and μ such that $|\psi\rangle = \lambda|\alpha_0\rangle|\beta_0\rangle + \mu|\alpha_1\rangle|\beta_1\rangle$. $\square$
(For a simple proof, let $|\psi\rangle = \sum_{ij} a_{ij}|ij\rangle$ be any state and just replace the matrix $[a_{ij}]$ by its singular value decomposition).
Assuming this theorem is true, prove that any 2-qubit state can be manufactured from $|0\rangle|0\rangle$ by application of a circuit comprising only 1-qubit gates and a *single* use of the 2-qubit CX gate.

(8) (Making controlled quantum oracles)
Suppose we have a quantum gate, given as a black box or oracle, that implements a unitary operation U on n qubits. Using this black box we wish to implement the controlled$-U$ operation CU on $1+n$ qubits (defined by $CU|b\rangle|\xi\rangle = |b\rangle U^b|\xi\rangle$ for $b = 0, 1$ and any n qubit state $|\xi\rangle$). Suppose we also have an n qubit state $|A\rangle$ with $U|A\rangle = |A\rangle$.
Introduce the n qubit controlled swap operation $CSWAP$ acting on $1+n+n$ qubits, defined by

$$CSWAP|b\rangle|\alpha\rangle|\beta\rangle = \begin{cases} |b\rangle|\alpha\rangle|\beta\rangle & \text{if } b = 0 \\ |b\rangle|\beta\rangle|\alpha\rangle & \text{if } b = 1 \end{cases}$$

(a) Show that $CSWAP$ is unitary.
(b) By considering a suitable circuit of $CSWAP$ and U gates show how CU may be implemented on $1+n$ qubit lines. [Hint: consider also using an extra ancillary n qubit register containing

$|A\rangle$.] Your construction must correctly apply CU to all superposed inputs of the $1+n$ qubit lines, not just those with $|b\rangle$ being $|0\rangle$ or $|1\rangle$.
(c) If U, now on $n+m$ qubits, is the standard quantum oracle U_f for a Boolean function $f : B_n \to B_m$, show that one application of CU_f may be implemented with one use of U_f.

(9)* (Hidden translation problem)
Suppose you are given two *bijective* functions $f_0 : B_n \to B_n$ and $f_1 : B_n \to B_n$ as quantum oracles (in the usual way). It is promised that there is a nonzero string $u \in B_n$ such that for all x we have $f_0(x) = f_1(x \oplus u)$. Give a quantum algorithm that finds u with bounded error probability and makes only $O(n)$ queries to the oracles. [Hint: consider a suitable larger oracle incorporating both f_0 and f_1, to which Simon's algorithm may be applied, and then think about how that oracle may be implemented using the given quantum oracles – here 8(c) may be useful.]

(10) (Period finding algorithm)
Suppose we want to factor $N = 39$ and we have chosen $a = 5$ so $f(x) = 5^x \bmod 39$.
(a) What is the number m of qubits used in the x-register in Shor's quantum factoring algorithm?
(b) Determine the period r of f, showing that in this case, f is exactly periodic on the full finite domain used.
(c) Suppose we construct the equal superposition state $|f\rangle$ over the domain of $0 \le x < 2^m$, measure the second register, perform the quantum Fourier transform $\bmod 2^m$ and finally measure the resulting state. What is the probability for each possible outcome $0 \le c < 2^m$? (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?

QUANTUM COMPUTATION – EXERCISE SHEET 2

Richard Jozsa rj310@cam.ac.uk (October 2016)

(1) (Shor's algorithm)
Suppose we wish to factor $N = 85$ and we have chosen $a = 3$. Show that a and N are coprime and compute the period r of $f(x) = a^x \bmod N$. Using r carry out the (classical) steps of the quantum factoring algorithm that lead to a factor of $N = 85$.

(2) (Shor's algorithm, continued fractions)
Suppose 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.
(d) Use your value of r to find factors of 21.

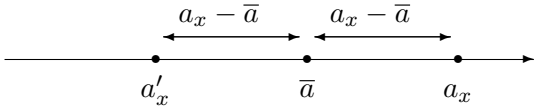
(3) (Rotation in Grover's algorithm)
For the plane $\mathcal{P}(x_0)$ spanned by $|x_0\rangle$ and $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{\text{all}x} |x\rangle$ set up an orthonormal basis in the plane. Then using the basis, show algebraically (rather than geometrically as in lectures) that the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

(4) (Grover's algorithm with an arbitrary starting state)
Consider Grover's algorithm in the case of a unique good item x_0 in a search space of size N. Suppose that instead of the usual uniform superposition state $|\psi_0\rangle$ we start with some other arbitrary 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 very close to 1. If we instead begin with some other starting state $|\eta_0\rangle$, give an expression for the probability of obtaining x_0 in the final measurement. Show that this may be improved by changing the number of Grover iterations. Describe geometrically how $|\eta_0\rangle$ evolves in the course of the computation.

(5) (An algebraic interpretation of Grover's algorithm)
(a) Consider the operator $-I_{|\psi_0\rangle} = 2|\psi_0\rangle\langle\psi_0| - I$ with $|\psi_0\rangle$ as in question (1) 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 $x = x_0$.

(6) (Gate presision and approximate QFT)
Often quantum gates cannot be implemented precisely. Let us define the distance $E(U, V)$ between two unitaries U and V as the maximum value of $||(U - V)|\psi\rangle||$ where the maximum is taken over all vectors $|\psi\rangle$ of length one i.e. $\langle\psi|\psi\rangle = 1$.

(a) Show that this distance is sub-additive i.e. prove that $E(U_1U_2, V_1V_2) \leq E(U_1, V_1)+E(U_2, V_2)$ for any four unitaries U_1, U_2, V_1, V_2.
(b) By looking at the circuit of QFT given in lecture notes (and the obvious generalisation to n qubit lines) show how to construct a circuit that approximates QFT mod $\mathbb{Z}_{2^n}$ to within $1/p(n)$ for any given polynomial $p(n)$ using only $O(n \log n)$ gates (recalling that in the original exact circuit we have $O(n^2)$ gates). Hint: most R_k are close to the identity.
(c) Argue that the appproximate circuit (for suitable $p(n)$) can be used in any BQP algorithm that uses QFT to slightly reduce the time complexity. (Hint: recall from the lecture on lower bounds on quantum search that if $||\,|\psi_1\rangle - |\psi_2\rangle\,|| \leq \epsilon$ then for any measurement, the probability distributions p_1 and p_2 obtained from $|\psi_1\rangle$ and $|\psi_2\rangle$ are related by $\sum_x |p_1(x) - p_2(x)| \leq 2\epsilon$.)

(7) (MQC J-lemma)
Prove the J-lemma of the measurement-based quantum computing formalism.

(8) (Circuit to MQC pattern)
Consider the following circuit on two qubits initially in state $|+\rangle_1 |+\rangle_2$: apply $J_1(\alpha_1)$ then $J_2(\alpha_2)$ then CZ_{12} then $J_1(\alpha_3)$. Finally measure both qubits in the computational basis to obtain output 2-bit string i_1i_2.
Express this computation as a measurement-based computation on an appropriate graph state. What is the logical depth of the measurement pattern?

(9) (Clifford computations and MQC)
The 1-qubit Pauli group $\mathcal{P}_1$ comprises I, X, Z, XZ together with their multiples by ± 1 and $\pm i$. The n-qubit Pauli group $\mathcal{P}_n$ is the n-fold tensor power $\mathcal{P}_1 \otimes \ldots \otimes \mathcal{P}_1$.

An n-qubit unitary operation C is called a *Clifford operation* if it has the following property: for any $P_1 \otimes \ldots \otimes P_n \in \mathcal{P}_n$ we have

$$C\,(P_1 \otimes \ldots \otimes P_n)\,C^\dagger = (P'_1 \otimes \ldots \otimes P'_n)$$

for some $P'_1 \otimes \ldots \otimes P'_n \in \mathcal{P}_n$ i.e. $\mathcal{P}_n$ is preserved under conjugation by C. Stated more formally, the group of all n-qubit Clifford operations is the group-theoretic normaliser of $\mathcal{P}_n$ in $U(2^n)$.

(a) H, the phase gate $P(\pi/2)$ and CZ are all Clifford operations. Check a few cases of choices of P_i's in the above and identify the corresponding P'_j's. (In fact it is a theorem that C is a Clifford operation on n qubits *if and only if* C can be expressed as a circuit of H, $P(\pi/2)$ and CZ gates).
(b) Show that any circuit of these three gates can be simulated by a measurement-based computation with logical depth 1. (Hint: first express H and $P(\pi/2)$ in terms of suitable $J(\alpha)$'s and then use the Clifford property to establish non-adaptive commutation relations for propagation of X and Z errors.)

(10) (Stabiliser formalism for graph states) (optional extra question, can be omitted)
Let $|Cl\rangle$ be the cluster state for an $n \times n$ grid D of qubits. Let V be the set of vertices of D, and let $|V| = n^2$ be the size of V.
(*Everything in this question can be easily generalised to the graph state $|\psi_G\rangle$ for any graph G but we'll consider just $|Cl\rangle$ on D for clarity/definiteness.*)
For any vertex a of D let $nbd(a)$ denote the set of its neighbours i.e. $b \in nbd(a)$ iff vertices a and b are connected by an edge of D.
A state $|\psi\rangle$ is said to be stabilised by an operator S if $S|\psi\rangle = |\psi\rangle$ i.e. $|\psi\rangle$ is a $+1$ eigenstate of S.

(i) Suppose $|\psi\rangle$ is stabilised by S. Show that $U|\psi\rangle$ (for unitary U) is stabilised by $USU^\dagger$.

(ii) Let $|P\rangle$ be the state of $|V|$ qubits obtained by placing a qubit in state $|+\rangle$ at each vertex of D. Show that $|P\rangle$ is stabilised by $X_{(a)}$ for each $a \in V$. Here, for any 1-qubit operator W, $W_{(a)}$ denotes the gate W applied to the qubit at a and the identity I at all other vertices.

(iii) Introduce the operator (for each $a \in V$) $K_a = X_{(a)} \bigotimes_{b \in nbd(a)} Z_{(b)}$ which acts non-trivially only on qubits in $nbd(a) \cup \{a\}$. Show that the eigenvalues of K_a are ± 1 only. Show that $|Cl\rangle$ is stabilised by K_a for each $a \in V$.
(Hint: consider how $|Cl\rangle$ is obtained from $|P\rangle$ and then use (i) together with the commutation relations, for all $a, b, c \in V$, of $X_{(c)}$ and $Z_{(c)}$ with $E_{(ab)} = CZ_{(ab)}$ that we had in lectures.)

We now aim to show that $|Cl\rangle$ is the *unique* quantum state (i.e. unit vector up to overall phase) that is stabilised by all the $2^{|V|}$ operators K_a.

(iv) Let $\{k_c\}$ be any set of bit values 0,1 labelled by $c \in V$. Show that there exists a state $|\psi_{\{k_c\}}\rangle$ of $|V|$ qubits satisfying (for all $a \in V$):

$$K_a |\psi_{\{k_c\}}\rangle = (-1)^{k_a} |\psi_{\{k_c\}}\rangle .$$

Here k_a is the element of the set $\{k_c\}$ for the vertex a. (Hint: we already have $|Cl\rangle$ for the k_c's all being 0, and consider (i) yet again).

(v) Show that the states $|\psi_{\{k_c\}}\rangle$ are orthogonal for different sets $\{k_c\}$.
(Hint: recall that $\langle\alpha| U |\beta\rangle$ is the inner product of $|\alpha\rangle$ with $U|\beta\rangle$ and also of $U^\dagger|\alpha\rangle$ with $|\beta\rangle$.)
Hence or otherwise deduce that $|Cl\rangle$ is the unique state (up to overall phase) satisfying $K_a|Cl\rangle = |Cl\rangle$ for all $a \in V$.

Remarks: All the above easily generalises to D being replaced by any graph G and $|Cl\rangle$ by the graph state $|\psi_G\rangle$. In general a stabiliser description of a state $|\alpha\rangle$ is a set of operators $\{S_i\}$ such that $|\alpha\rangle$ is stabilised by them all and also is the *unique* such state. Thus the set of operators $\{K_a : a \in V\}$ is a stabiliser description of $|\psi_G\rangle$. It is an *efficient* (i.e. poly($|V|$)-sized) description even though $|\psi_G\rangle$ involves exponentially many (i.e. $2^{|V|}$) amplitudes. This makes it very useful for some purposes – it can provide efficient classical simulations of some MQC processes, and it can provide alternative (sometimes simpler/elegant) derivations of properties of the graph state $|\psi_G\rangle$ and features of MQC processes.

(vi) (optional) Suppose that the qubit of $|Cl\rangle$ at vertex a of D is measured (in the computational basis) giving the result 0 (i.e. this qubit is collapsed to $|0\rangle$ after measurement). Let H be the graph obtained from D by deleting the vertex a and all edges to it.
Using the stabiliser description (and recalling that $(I + Z)/2$ is the 1-qubit operation of projection onto $|0\rangle$), show that the post-measurement state of the qubits of H is the graph state $|\psi_H\rangle$ on the graph H.

QUANTUM COMPUTATION – EXERCISE SHEET 3

Richard Jozsa rj310@cam.ac.uk (October 2016)

(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. The issue is that the Grover iteration operator's rotation angle 2θ is not generally an exact integer fraction of the full angle between the starting state and its good component. However Grover search (and AA) can be modified to work with probability 1, as follows.

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

$$|\psi\rangle = \alpha\,|\psi_g\rangle + \beta\,|\psi_b\rangle$$

where as usual, α and β are real and positive, and $|\psi_g\rangle$ and $|\psi_b\rangle$ 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. 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 if we are given $|\psi\rangle$ and any $\alpha' < \alpha$, we can construct a state $|\phi\rangle$ of the extended system with

$$|\phi\rangle = \alpha'\,|\phi_g\rangle + \beta'\,|\phi_b\rangle\,.$$

Here $|\phi_g\rangle$ resp. $|\phi_b\rangle$ are normalised superpositions of extended good resp. bad labels.

(b) Show that the AA process in (a) can be made exact - i.e. the final measurement will yield a good x with certainty - by using at most one extra query to Q.

(2) (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.

(3) (Factoring via phase estimation)
Fix two coprime positive integers x and N such that $x < N$, and let U_x be the unitary 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 $x^t \equiv 1$). For $0 \leq s \leq r-1$, define the states

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

(a) Verify that U_x is indeed unitary.

(b) Show that, for arbitrary integers $n \geq 0$, $U_x^{2^n}$ can be implemented in time poly (n) (not poly (2^n)!).

(c) Show that each state $|\psi_s\rangle$ is an eigenvector of U_x with eigenvalue $e^{2\pi i s/r}$.

(d) Show that

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\psi_s\rangle = |1\rangle .$$

(e) Thus show that, if the phase estimation algorithm with n qubits is applied to U_x using $|1\rangle$ in place of the input of a genuine eigenvector, then the algorithm outputs (with constant probability) an estimate of s/r accurate up to n bits, for $s \in \{0, \ldots, r-1\}$ picked uniformly at random. (You may quote any appropriate theorems from the lectures).

(f) Argue that the above phase estimation algorithm can be used to factorise an integer N in poly $(\log N)$ time (Kitaev's quantum factoring algorithm).

(4) (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 quantum circuit running in time poly (n), and $D = \sum_x d(x) |x\rangle \langle x|$ is a diagonal matrix such that the map $|x\rangle \mapsto e^{-id(x)t} |x\rangle$ can be implemented in time poly (n) for all x. Show that e^{-iHt} can be implemented in time poly (n).

(5) (Quantum oracle interrogation) (an optional extra)
In this question we'll prove the following result of Wim van Dam.
Theorem A: Given oracle access to the bits of an unknown n-bit string x, there is a quantum algorithm that learns x completely with success probability at least 0.999 using $n/2 + O(\sqrt{n})$ queries, for any x.

"Oracle access to the bits of x" means that we have a standard quantum oracle for the function $f_x : \{1, 2, \ldots, n\} \to B_1$ with $f_x(k) =$ the k^{th} bit of x.

The success probability 0.999 can in fact be taken to be any constant strictly less than 1. It can be shown that classically we need a full n queries to learn x with any worst-case success probability exceeding a half (Why?)

(a) Show that, for any $x \in \{0,1\}^n$, given the n qubit state $|\psi_x\rangle := \frac{1}{2^{n/2}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$, there is a quantum algorithm that determines x with certainty using no additional queries to the bits of x. (Here $x \cdot y = \sum_i x_i y_i$ is the inner product of x and y modulo 2.)

(b) For any $0 \leq r \leq n$, consider the state

$$|\psi_x^r\rangle := \frac{1}{\sqrt{R}} \sum_{y \in \{0,1\}^n, |y| \leq r} (-1)^{x \cdot y} |y\rangle ,$$

where $R = \sum_{i=0}^{r} \left(\begin{array}{c} n \\ i \end{array} \right)$, and for any bit string y, $|y|$ denotes its Hamming weight i.e. the number of 1's in y. Show that, for some $r = n/2 + O(\sqrt{n})$, $|\langle \psi_x | \psi_x^r \rangle|^2 \geq 0.999$. [Hint: look up the Chernoff bound for sums of binomial coefficients.]

(c) Show that the state $|\psi_x^r\rangle$ can be produced using r queries to bits of x.

(d) Use parts (a) (b) and (c) to prove theorem A.