Part III QUANTUM COMPUTATION
EXERCISE SHEET 1

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

Questions 4 and 7 are optional and can be left to the end if you have time.

(1) (Shift invariant states)
Let G be any finite abelian group.
(i) Show that for any irrep χ and $g \in G$, $\chi(g)$ is a $|G|^{\text{th}}$ root of unity.
(ii) Show that the associated shift invariant states $|\chi\rangle = \frac{1}{\sqrt{|G|}} \sum_{g\in G} \overline{\chi(g)}\, |g\rangle$ form an orthonormal set. [Hint: for an elementary proof it may help to consider suitably re-expressing the expression $\chi_i(h) \sum_{g\in G} \chi_i(g)\overline{\chi_j(g)}$ where χ_i and χ_j are any two irreps.]

(2) (Generalised Simon's problem)
Suppose we have an oracle for a function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ which is promised to be a 2^k-to-1 function of the following particular form – there exist k (linearly independent in $\mathbb{Z}_2^n$) n-bit strings $a_1, \ldots, a_k \in \mathbb{Z}_2^n$ with $f(x) = f(x \oplus a_i)$ for all $x \in \mathbb{Z}_2^n$ and $i = 1, \ldots, k$ (and here $\oplus$ denotes bitwise addition of n-bit strings at each position separately). The problem is to output any $b \in \mathbb{Z}_2^n$ having $f(x) = f(x \oplus b)$ for all $x \in \mathbb{Z}_2^n$. (The case $k = 1$ is the original Simon's problem).

(a) Show how the problem may be formulated as an abelian HSP. Find the associated shift invariant states and determine the associated Fourier transform on the group.

(b) Show that if m m-bit strings $x_1, \ldots, x_m$ are chosen uniformly randomly and independently from $\mathbb{Z}_2^m$ then they will be linearly independent (under the $\oplus$ addition) and not include the all-zero string $000\ldots0$, with probability at least $\frac{1}{4}$.
Hint: note that

$$\prod_{j=1}^{m} \left(1 - \frac{2^{j-1}}{2^m}\right) = \frac{1}{2} \prod_{j=1}^{m-1} \left(1 - \frac{2^{j-1}}{2^m}\right)$$

and that for a and b in $[0,1]$ we have $(1-a)(1-b) \geq 1 - (a+b))$.

(c) Using the result of (b) and the formulation in (a), show that in the standard quantum algorithm for the abelian HSP, $n-k$ queries to the oracle for f suffice to solve the generalised Simon's problem with probability at least $\frac{1}{4}$.

(d) Show that the problem may be solved with probability $1-\epsilon$ for any specified $\epsilon > 0$, however small, with $O(n)$ queries.

(3) (Graph isomorphism and swap test)
(A GI quantum algorithm idea that didn't work.)
(a) The *swap test* is a procedure for determining whether two given states $|\alpha\rangle$ and $|\beta\rangle$ in $\mathcal{H}_d$ are close or far apart: adjoining an extra qubit $\mathcal{H}_2$ we'll work in $\mathcal{H}_2 \otimes \mathcal{H}_d \otimes \mathcal{H}_d$ starting with state $|0\rangle\,|\alpha\rangle\,|\beta\rangle$, and apply the following sequence of actions: first the Hadamard gate H to the qubit, then the controlled SWAP gate (controlled by the qubit), then H to the qubit again (the SWAP gate on $\mathcal{H}_d \otimes \mathcal{H}_d$ maps $|\alpha\rangle\,|\beta\rangle$ to $|\beta\rangle\,|\alpha\rangle$ for any $|\alpha\rangle$, $|\beta\rangle \in \mathcal{H}_d$).
Finally measure the qubit and output 'near' if the result is 0, and output 'far apart' if the result is 1.

Show that the probability of result 0 is $(1 + |\langle\alpha|\beta\rangle|^2)/2$. Deduce that for the case where $|\alpha\rangle$ and $|\beta\rangle$ are promised a priori to be either the same or orthogonal, the output ('near' or 'far apart') is always correct if $|\alpha\rangle = |\beta\rangle$ and correct with probability half if the states were orthogonal.

(b) Consider the graph isomorphism problem (GI) for graphs with n vertices, that are undirected with at most one edge between any two vertices, and having vertices labelled by $[n] = \{1, 2, \ldots, n\}$. Any such graph A is conveniently specified by its $n \times n$ *adjacency matrix* M_A having entries $[M_A]_{ij} = 1$ if there is an edge between i and j, and 0 otherwise. If π is any $n \times n$ permutation matrix then the graph $\pi(A)$, obtained by permuting the vertex labels of A by π, has $M_{\pi(A)} = \pi M_A \pi^T$ (where T denotes transpose). Let $\mathcal{P}_n$ denote the group of permutations of $[n]$ and let X be the set of all labelled graphs (adjacency matrices). For any A introduce $f_A : \mathcal{P}_n \to X$ having $f_A(\pi) = \pi(A)$.

Using the associated quantum oracle U_{f_A} we can readily create the state

$$|\xi_A\rangle = \sum_{\pi \in \mathcal{P}_n} |\pi\rangle \, |\pi(A)\rangle$$

(where we are omitting overall normalisation factors). Suppose we were able to "erase" or "forget" the content of the first register (e.g. reset it to some fixed π_0 independent of the second register) and obtain the state representing the superposition of just the f_A values by themselves:

$$|\eta_A\rangle = \sum_{\pi \in \mathcal{P}_n} |\pi(A)\rangle \, .$$

Show (considering the swap test) that we could then solve the graph isomorphism problem for two such graphs A and B.

(4) ((a) Graph isomorphism as an HSP, and (b) as a balanced-vs-constant problem) (optional; if time permits)
(More GI quantum algorithm ideas that didn't work.)
(a) Recall the HSP for the automorphism group $\mathrm{Aut}(S)$ for any labelled graph S on n vertices: the group is $\mathcal{P}_n$ and the hiding function is f_S (as defined in question 3(b)). Let A and B be any two graphs of the kind in question 3(b) that are also connected graphs (i.e for any pair (i, j) of vertices, there is a path of edges from i to j).
(i) In terms of M_A and M_B write down a condition that $\pi \in \mathcal{P}_n$ is in $\mathrm{Aut}(A)$, and that A and B are isomorphic graphs (written $A \cong B$).
(ii) Consider the graph C on $2n$ vertices that is the disjoint union of A and B labelled by $[2n] = \{1, 2, \ldots, 2n\}$ with $L_A = \{1, 2, \ldots, n\}$ labelling A and $L_B = \{n + 1, \ldots, 2n\}$ labelling B. We have $\mathrm{Aut}(C) \subseteq \mathcal{P}_{2n}$.
Show that any $\pi \in \mathrm{Aut}(C)$ must either:
(P1): swap the sets L_A and L_B fully, or
(P2): permute L_A and L_B separately into themselves.
Show that if $A \cong B$ then exactly half of the elements of $\mathrm{Aut}(C)$ satisfy each of (P1) and (P2), and that if $A \ncong B$ then all elements of $\mathrm{Aut}(C)$ satisfy (P2).
Conclude that we can reduce the GI problem for A and B to the HSP for graph automorphism (where the output of the HSP algorithm is a uniformly random element of the hidden subgroup).

(b) Let B_n denote the set of all n-bit strings. Consider the *partial* balanced-vs-constant problem: We have an oracle for a function $f : B_n \to B_1$ and we are given a uniform superposition state of some subset $S \subseteq B_n$ of n-bit strings $|\alpha\rangle = \frac{1}{\sqrt{|S|}} \sum_{x \in S} |x\rangle$ with $|S|$ even. It is promised that f restricted to the domain S is either balanced (in the sense that exactly half of its $|S|$ values are 0 resp. 1) or constant, and we wish to determine which one is the case.
(i) Recall (e.g. write down how): in the case that $S = B_n$, this can be solved on a quantum computer with a single query to the oracle and $O(n) = O(\log(2^n))$ further processing time.
(ii) Let $\sigma \in \mathcal{P}_{2n}$ be the permutation that swaps L_A and L_B in their listed order (as above). Consider the group $G = (\mathcal{P}_n \times \mathcal{P}_n) \cup \sigma(\mathcal{P}_n \times \mathcal{P}_n) \subset \mathcal{P}_{2n}$ which has $\log |G| = O(\mathrm{poly}(n))$. For the graph C as in (a) note that $\mathrm{Aut}(C) \subseteq G$. By considering the function $f_C(\pi) = \pi M_C \pi^T$ on domain G, show that an efficient (i.e. poly(n) time) quantum algorithm for the partial

balanced-vs-constant problem above would give an efficient solution of the graph isomorphism problem.
(Hint: consider $f : G \to B_1$ with $f(\pi) = 0$ if $\pi \in \mathcal{P}_n \times \mathcal{P}_n$ and $f(\pi) = 1$ if $\pi \in \sigma(\mathcal{P}_n \times \mathcal{P}_n)$; and you may assume that f_C is efficiently implementable).

(5) (Implementing M^{th} root operations)
For any given positive integer M and unitary U, let $U^{1/M}$ denote the principal M^{th} root of U defined to have the same eigenstates as U and corresponding eigenvalues given by $e^{2\pi i\phi/M}$ where $e^{2\pi i\phi}$ with $0 \leq \phi < 1$ are the eigenvalues of U. Suppose that each ϕ has the form $y/2^n$ for a corresponding integer $0 \leq y < 2^n$.
If $\phi = y/2^n$ with $y = i_1 i_2 \ldots i_n$ in binary, show that

$$\frac{2\pi\phi}{M} = i_1\frac{2\pi}{2M} + i_2\frac{2\pi}{4M} + \ldots + i_n\frac{2\pi}{2^n M}.$$

Suppose now that we are given a quantum oracle for the controlled U gate c-U and its inverse c-U^{-1}. We also have an exactly universal set of quantum gates available, so in particular we are able to exactly implement any desired phase gate $P(\alpha) = \text{diag}(1\ \ e^{i\alpha})$. By considering the unitary part of the Phase Estimation algorithm, explain how we can then implement the gate $U^{1/M}$ on any d-dimensional state $|\xi\rangle$.

(6) (Implementing non-unitary operations)
Let A be an n-qubit Hermitian operator with all eigenvalues λ_i distinct and each having the form $\lambda_i = c_i/2^n$ for an integer $0 \leq c_i < 2^n$. Suppose further that for the unitary operations $U_\pm = e^{\pm 2\pi i A}$ we are able to implement the controlled versions c-$U_\pm$ (on $n+1$ qubits). We are given an n-qubit state $|b\rangle$ (as a quantum physical state, with its actual identity possibly unknown) and we wish to produce the state $|\psi\rangle$ given by the vector $A\,|b\rangle$ normalised, with some non-zero probability. We have available a universal set of gates and in particular we are also able to implement controlled rotations of the form

$$|c\rangle\,|0\rangle \longrightarrow |c\rangle\,(\cos\theta_c\,|0\rangle + \sin\theta_c\,|1\rangle)$$

where $0 \leq c < 2^n$ is an integer and $\sin\theta_c = c/2^n$. Here the first and second registers are an n-qubit and one-qubit register respectively.

Let $|u_j\rangle$ be a normalised eigenvector of A belonging to λ_j, and let $|b\rangle = \sum \beta_j\,|u_j\rangle$. Show how we can construct the state

$$\sum \beta_j\sqrt{1-\lambda_j^2}\,|u_j\rangle\,|c_j\rangle\,|0\rangle + \beta_j\lambda_j\,|u_j\rangle\,|c_j\rangle\,|1\rangle$$

from $|b\rangle$. Here the first two registers are each n-qubit registers and the third is a one-qubit register. Hence (or otherwise) show how the state $|\psi\rangle$ may be obtained with probability of success exceeding the square of the smallest eigenvalue of A.

(7) (General non-abelian HSP query complexity)(optional; if time permits)
Let G be any finite group and $f : G \to X$ a function that is constant and distinct on the cosets of a 'hidden' subgroup $K \leq G$. Write

$$|gK\rangle = \frac{1}{\sqrt{|K|}}\sum_{k\in K}|gk\rangle\,.$$

With m queries to the quantum oracle for f we can prepare the product of m coset states

$$|\psi\rangle = |g_1K\rangle\,|g_2K\rangle\ldots|g_mK\rangle \tag{1}$$

where $g_1,\ldots,g_m$ have been chosen independently and uniformly randomly from G. We aim to show that $m = O(\text{poly}(\log|G|))$ random coset states suffice to determine K with any desired probability $1-\epsilon$, $\epsilon > 0$. However the processing of $|\psi\rangle$, that we will develop to identify K, will require exponential time in $\log|G|$ so we do not get an efficient algorithm for the HSP despite having an efficient query complexity.

(a) (i) If K and K' are two subgroups of G show that any coset intersection $gK \cap g'K'$ is either empty or it contains $|K \cap K'|$ elements of G.
(ii) Note that distinct coset states of any subgroup K are orthogonal and there are $|G|/|K|$ of them. Let P_K denote the orthogonal projection onto the linear span of all these $|G|/|K|$ coset states $|gK\rangle$, $g \in G$. Show that

$$||P_{K'}\,|gK\rangle\,||^2 = \frac{|K \cap K'|}{|K'|}.$$

Deduce that:
$P_{K'}\,|gK\rangle = |gK\rangle$ if K' is a subgroup of K, and
$||P_{K'}\,|gK\rangle\,|| \leq 1/\sqrt{2}$ if K' is not a subgroup of K.

Let $P_K^{(m)} = (P_K)^{\otimes m}$ denote the orthogonal projector onto the linear span $V_K^{(m)}$ of all product states of the form eq. (1). Then we have

$$||P_{K'}^{(m)}\,|\psi\rangle\,|| \leq \frac{1}{2^{m/2}} \quad \text{if } K' \text{ is not a subgroup of } K. \tag{2}$$

Convince yourself that this gives the following:
if the actual hidden subgroup is K and we make an incomplete measurement $\mathcal{M}_{K'}^{(m)}$ on $|\psi\rangle$ relative to the orthogonal subspaces $\{V_{K'}^{(m)}, V_{K'}^{(m)\perp}\}$ with outcomes labelled 0 and 1 respectively, then
if $K' \leq K$ then prob(0) $= 1$, and
if $K' \nleq K$ then prob(0) $\leq 1/2^m$.

(b) Now in terms of the above, our HSP algorithm is as follows. Make a list $K_1, K_2, \ldots, K_R$ of all candidate hidden subgroups, in any order of non-increasing size $|K_i|$. Hence no K_r in the list is a subgroup of any K_s with $s > r$. Then given $|\psi\rangle$ as in eq. (1), we perform the sequence of measurements $\mathcal{M}_{K_1}^{(m)}, \mathcal{M}_{K_2}^{(m)}, \ldots$ on it, continuing until outcome 0 is obtained for the first time. The corresponding K_r is identified as the hidden subgroup K.
Note that in this process each measurement will successively disturb the state, projecting it into the subspace corresponding to the seen outcome, so the input state $|\psi\rangle$ becomes increasingly altered as the process proceeds.

Despite this accumulating disturbance we can see that the algorithm solves the HSP with good probability, as follows.
If the actual hidden subgroup is K_r in the list, show that the probability of successful identification is

$$P_{\text{success}} = ||P_{K_r}(I - P_{K_{r-1}}) \ldots (I - P_{K_1})\,|\psi\rangle\,||^2.$$

Next note (i.e. convince yourself) that for any projection operators A, B and any state $|\xi\rangle$ we have $||A\,|\xi\rangle - A(I-B)\,|\xi\rangle\,|| = ||AB\,|\xi\rangle\,|| \leq ||B\,|\xi\rangle\,||$ and deduce that

$$P_{\text{success}} \geq \left(1 - \frac{(r-1)}{2^{m/2}}\right)^2.$$

Conclude that the algorithm can be made to have any prescribed success probability $1-\epsilon$ by taking $m = O(\log r)$.
Now (as you may assume without proof) any subgroup of G is generated by a set of at most $\log|G|$ elements. Deduce that $R \leq |G|^{\log|G|} = 2^{(\log|G|)^2}$, and hence conclude that $m = O(\log R) = O((\log|G|)^2)$ coset states suffice to determine K in every case, although the process may involve as many as $2^{(\log|G|)^2}$ measurements i.e. exponentially many, before finishing.