**Part III QUANTUM COMPUTATION**
**EXERCISE SHEET 3**

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

**(1) (approximate gates, accumulation of errors)**
(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 $||U_2U_1 - V_2V_1|| \leq \epsilon_1 + \epsilon_2$ i.e. errors in using approximate versions at most add when gates are composed.
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) The 1-qubit gate $J(\alpha)$ is given by

$$J(\alpha) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix}$$

and $\{J(\alpha), CZ\}$ is known to be a universal set of gates.
In a laboratory we wish to implement a circuit $C$ of $J(\alpha)$ and $CZ$ gates containing $k$ $J(\alpha)$ gates. The laboratory is able to perform $CZ$ gates exactly but, due to difficulties with continuous variables, for each $J(\alpha)$ gate, the actual implemented gate is $J(\alpha')$ for some $\alpha'$ with $|\alpha' - \alpha| < \eta$. If $|\psi_{\text{in}}\rangle$ is the input state let $|\psi_{\text{out}}\rangle = C\,|\psi_{\text{in}}\rangle$ denote the output state of the exact circuit, and let $|\psi'_{\text{out}}\rangle$ denote the output state of the implemented circuit. We require that $||\,|\psi_{\text{out}}\rangle - |\psi'_{\text{out}}\rangle\,|| < \epsilon$ (where $||\,|\xi\rangle\,||$ denotes the usual vector length). Determine a (non-zero) bound on $\eta$ that suffices to guarantee the required condition on the output state.

**(2) (HHL application)**
A discrete linear dynamical system $\mathcal{L}$ has state vector $x_t \in \mathbb{R}^N$ with $t = 0, 1, 2, \ldots$ and evolution rule $x_{t+1} = \mathcal{L}x_t = Ax_t + b$ specified by an $N \times N$ matrix $A$ and constant $b \in \mathbb{R}^N$. Suppose further that $A$ is hermitian and $||A|| \leq 1/2$, and the system has been scaled to have $||b|| = 1$. The stable state of $\mathcal{L}$ is $s \in \mathbb{R}^N$ with $\mathcal{L}s = s$.

Suppose we are given two such dynamical systems $(A, b)$ and $(A', b')$ with the promise that their stable states $s$ and $s'$ are either (a) within angle $\pi/6$ of each other, or (b) further than angle $\pi/3$ apart. We wish to decide which of (a) or (b) is the case.

Show how the HHL algorithm may be used to solve this problem with probability $1 - \epsilon$ for any $\epsilon > 0$, in poly$(\log N)$ time, stating also any further conditions on the defining ingredients that are needed. (This is exponentially faster than any known classical method).

**(3) (the controlled rotation in HHL)**
The HHL algorithm for a linear system of size $N$ uses a 1-qubit rotation controlled by a poly$(\log N)$ qubit register as follows:

$$C_{\text{rot}} : |\lambda\rangle\,|0\rangle \to |\lambda\rangle\,(\cos\theta_\lambda\,|0\rangle + \sin\theta_\lambda\,|1\rangle)\,. \tag{1}$$

Here the first register comprises poly$(\log N)$ qubits specifying the eigenvalue $\lambda$ which lies in the interval $[1/\kappa, 1]$ where $\kappa = O(\text{poly}(\log N))$ is the (known) condition number of the linear system, and $\theta_\lambda \in [0, \pi/2]$ is given by $\sin\theta_\lambda = C/\lambda$ for any chosen constant $C < 1/\kappa$. Write $m$ for poly$(\log N)$.

(a) Describe how the operation $C_{\text{rot}}$ on $m + 1$ qubits (and use of any further ancillary qubits if needed) can be expressed as an $O(m)$-sized circuit of 1- and 2-qubit gates. You may ignore any issues of precision that arise i.e. you may assume that the value of $\theta_\lambda$ may be classically exactly computed from $\lambda$ in $O(m)$ time and represented within $O(m)$ bits (which is in fact true for the value of $\theta_\lambda$ to $O(m)$ bits of precision).

(b) (optional) In fact $m$ qubits can represent $\lambda$ and $\theta_\lambda$ only to accuracy $O(1/2^m)$. Let $\tilde{C}_{\rm rot}$ be the approximation to $C_{\rm rot}$ that is obtained by giving $\lambda$ only to $O(1/2^m)$ accuracy and then computing $\theta_\lambda$ from it to $O(1/2^m)$ accuracy. Show that $||C_{\rm rot} - \tilde{C}_{\rm rot}|| \leq O(\text{poly}(m)/2^m)$ and deduce that this error can be made arbitrarily small while retaining $m = O(\text{poly}(\log N))$ qubits in the quantum computation.

**(4) (optional; if time permits) (HHL RHS state preparation)**
We have available a universal set of 1- and 2-qubit gates $\mathcal{G}$ and assume (for simplicity) that any 1- or 2-qubit gate can be made exactly using a constant number of gates from $\mathcal{G}$.
(i) Given $a, b \geq 0$ real with $a^2 + b^2 = 1$, describe how the state $|\xi\rangle = a\,|0\rangle + b\,|1\rangle$ can be made from $|0\rangle$.
Further to $a, b$, introduce $s, t, u, v, \geq 0$ with $s^2 + t^2 = a^2$ and $u^2 + v^2 = b^2$, and describe how the state $|\eta\rangle = s\,|00\rangle + t\,|01\rangle + u\,|10\rangle + v\,|11\rangle$ can be made from $|00\rangle$ using a 1-qubit gate and a controlled rotation of the form $|x\rangle\,|\psi\rangle \to |x\rangle\,R(\theta_x)\,|\psi\rangle$ where $|\psi\rangle$ is any 1-qubit state, $x = 0, 1$ and $R(\theta)$ is rotation of a qubit by angle $\theta$ i.e. the two control settings $x = 0, 1$ induce different corresponding rotation angles on the target qubit.

(ii) Let $N = 2^n$. Let $b_1, b_2, \ldots, b_{N-1} \geq 0$ be such that $\sum_{i=0}^{N-1} b_i^2 = 1$ and such that

$$f(k) = b_k \quad \text{and} \quad g(k_1, k_2) = \sum_{i=k_1}^{k_2} b_i^2 \qquad \text{for any } 0 \leq k, k_1, k_2 \leq N-1$$

are efficiently (classically) computable i.e. in poly$(n)$ time. Show that the state $|b\rangle = \sum_{i=0}^{N-1} b_i\,|i\rangle$ may be made with poly$(n)$ time classical and quantum computation. You may ignore any issues of precision and assume that any needed quantities can be represented in $O(n)$ qubits.
Hint: consider iterating the construction above, and it may be be useful to recall a controlled rotation construction like that in question 3, which may here be assumed to be implementable in poly$(n)$ time (or you may like to prove that too).
Remark: the result may be generalised to $b_i \in \mathbb{C}$ with $\sum |b_i|^2 = 1$ and the corresponding $f$ and $g$ being efficiently computable.

**(5) (the 'linear combination of unitaries' method)**
We wish to implement an operation $A$ that is not necessarily unitary, so it cannot itself be directly viewed as a quantum operation.
(i) Show that any $d \times d$ matrix $A$ can be expressed as a linear combination of unitary matrices, involving no more than $d^2$ summands.
(ii) Consider the case of a linear combination of just two unitaries $U_0$ and $U_1$ on state space $\mathcal{H}_d$:

$$A = \alpha_0 U_0 + \alpha_1 U_1$$

where, without loss of generality (why?) $\alpha_0$ and $\alpha_1$ can be taken to be real and non-negative. Adjoin an extra qubit (control qubit) and suppose we can implement the controlled operation:

$$U = |0\rangle\langle 0| \otimes U_0 + |1\rangle\langle 1| \otimes U_1$$

i.e. apply $U_0$ resp. $U_1$ to $\mathcal{H}_d$ if the control is $|0\rangle$ resp. $|1\rangle$. Write $\alpha = \alpha_0 + \alpha_1$ and introduce the 1-qubit unitary

$$V_\alpha = \frac{1}{\sqrt{\alpha}} \begin{bmatrix} \sqrt{\alpha_0} & -\sqrt{\alpha_1} \\ \sqrt{\alpha_1} & \sqrt{\alpha_0} \end{bmatrix}.$$

For any $|\psi\rangle \in \mathcal{H}_d$, to implement '$A\,|\psi\rangle$ normalised' consider the sequence of operations: $V_\alpha \otimes I$, then $U$, then $V_\alpha^\dagger \otimes I$ on $|0\rangle\,|\psi\rangle$. Show that $A\,|\psi\rangle$ normalised can then be obtained by a suitable post-selected final measurement. Show that the probability of failure of the post-selection is $\leq 4\alpha_0\alpha_1/\alpha^2$.

**(6) (strong and weak classical simulations)**
To avoid precision issues, assume in this question that all probabilities have the form $c/2^m$ where $0 \leq c \leq 2^m$ is an integer and $m$ is polynomial in the number of qubit lines of the computation from which the probability arises. (The case of general probability values can be readily approximated to any desired accuracy in number of bits by similar methods).

(a) Suppose we have a classical computer that can also "toss a fair coin" i.e. sample the probability distribution $p_0 = p_1 = 1/2$ and have subsequent computational steps chosen depending on the result. Show that for a quantum computation with a single output line, efficient strong simulation implies efficient weak simulation.

(b) Suppose now that the quantum computation has $k$ output lines (where $k$ can be $O(n)$ for a circuit on $n$ qubits). In this scenario we strengthen the definition of strong simulation as follows: each $k$-bit output probability $p_{i_1 \ldots i_k}$ *and* each marginal output probability on $l < k$ lines can be classically efficiently computed. The definition of weak simulation remains as before (i.e. the ability to classically efficiently sample from the output distribution). Show that again (with this strengthened notion of strong simulation) efficient strong simulation implies efficient weak simulation.
Hint: Recall the Bayes rule formula that we used in Sheet 1 Q2, that
$P(A_1 A_2 \ldots A_k) = P(A_1)\, P(A_2|A_1) P(A_3|A_2 A_1) \ \ldots \ P(A_{k-1}|A_{k-2} \ldots A_1)\, P(A_k|A_{k-1} \ldots A_1)$.

(c) (optional, if you know a little about NP)
For the converse direction in (b): show that if the possibility of efficient weak simulation implies the possibility of efficient strong simulation, then P=NP.
Hint: consider SAT and a quantum circuit that evaluates a Boolean function $f$ :1-bit$\rightarrow n$-bits.

**(7) (adaptive and non-adaptive Clifford computations)**
(a) (equivalence of non-adaptive Clifford computations with fully unitary ones)
Let $|\psi\rangle_{123}$ be any 3-qubit state and $C, D$ Clifford operations, each on 3 qubit lines labelled 1,2,3. Consider the following two processes on $|\psi\rangle$ as input:
(P1): apply $C$, then measure line 3 (in the standard basis), then apply $D$ (to the 3-qubit post-measurement state). Finally measure line 1 to get output 0 or 1.
(P2): adjoin an extra ancilla qubit $|0\rangle_4$. Starting with $|\psi\rangle_{123}|0\rangle_4$ apply the sequence of unitary gates: $C_{123}$, then $CX_{34}$, then $D_{123}$. Finally measure the first qubit line of the resulting 4-qubit state to get output 0 or 1.

Show that the output probability distributions of processes (P1) and (P2) are the same i.e the non-adaptive process (P1) having an intermediate measurement is equivalent (for the output) to the fully unitary (P2). The method easily generalises to any number of non-adaptive intermediate measurements, by introducing a $|0\rangle$ ancilla for each one.

(b) (the $T$-gadget)
For any 3-qubit state $|\psi\rangle_{123}$, adjoin a fourth ancilla qubit in state

$$|A\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + e^{i\pi/4} |1\rangle \right).$$

Show (by a direct calculation) that the effect of the $T$-gadget (as given in lectures) applied to line 2 of $|\psi\rangle$ (i.e. using $CX_{24}$ in the gadget), always results in the application of the $T$ gate (up to an overall phase) to $|\psi\rangle$ on its second line (i.e. an action of $T_2$).