1. Kvantum-számításelmélet feladatsor (Richard Józsa feladatai)

(Beadási határidő: 2014.03.26. `www.cs.elte.hu/~pal/QC` e-mail: pal@cs.elte.hu)

(1) (Quantum teleportation) Write $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and let $|\alpha\rangle = a|0\rangle + b|1\rangle$ be a general 1-qubit state. Subscripts will denote qubit positions labelled from left to right, in a multi-qubit state.

(a) Write $|A\rangle_{123} = |\alpha\rangle_1 |\psi\rangle_{23}$ in the computational basis of three qubits and hence compute $|B\rangle_{123} = (H_1 \otimes I_{23})(CX_{12} \otimes I_3)|A\rangle_{123}$.

(b) Suppose we perform a standard quantum measurement on qubits 1 and 2 of $|B\rangle$. Show that the four possible outcomes $ij = 00, 01, 10, 11$ are always equiprobable and compute the post-measurement state in each case.

(c) Show that in each case the post-measurement state in slot 3 is a unitary transform of $|\alpha\rangle$ (independent of a and b) and identify the corresponding unitary matrix U_{ij} for each possible outcome ij.

Remark: in quantum teleportation Alice holds qubits 1 and 2 while Bob, distantly separated in space, holds qubit 3. So Alice, by applying the local operations H_1, CX_{12} and local measurements, can faithfully transfer the state of qubit 1 to Bob (even if she does not know its identity), at the communication expense of sending him only *two classical bits* ij (so he can correct the unitary "error" U_{ij}).

(2) (Basic entanglement) Prove that the state $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ is entangled iff $ad - bc \neq 0$. Deduce that the state $|\varphi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + (-1)^k|11\rangle)$ is entangled if $k = 1$

(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

(3) (No cloning of quantum states) We routinely copy classical data in everyday life e.g. for a single bit value $b = 0$ or 1, show that the classical CNOT gate (which operates just like the quantum CX gate on basis states viz. $(b, c) \mapsto (b, b \oplus c)$ for bits b, c) when acting on the 2-bit pair $(b, 0)$, will copy b into the second slot i.e. we get (b, b).

(i) Consider now the quantum CNOT gate acting on the 2-qubit state $|\psi\rangle|0\rangle$ where $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is a general qubit state. Will we now get a copy of $|\psi\rangle$ in the second register? i.e. do we get $|\psi\rangle|\psi\rangle$?

(ii) Consider *any* process which purports to clone an arbitrary input qubit state. Any such process has the following form. The input is $|\psi\rangle|0\rangle \ldots |0\rangle$ where $|\psi\rangle$ is any qubit state and $|0\rangle \ldots |0\rangle$ are any required number of "working space" qubits all in state $|0\rangle$. The output is $|\psi\rangle|\psi\rangle|A_\psi\rangle$ i.e. we get two copies of $|\psi\rangle$ together with (possibly) some further ψ-dependent state $|A_\psi\rangle$. Prove that no such process can exist within the framework of quantum theory i.e. "quantum states cannot be cloned". (Hint: think about unitarity).

(4) (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).

(A szorzás, összeadás, stb. alapműveletek természetesen mind polinomiális időben kiszámíthatóak. Vagyis igazából azt kell megmutatni, hogy a folyamat jól szimulálható összesen polinomiális sok alapművelet elvégzésével – és közben végig elég polinomiális (bit)méretű számokkal számolni.)

(5) (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 $a = a_1 \ldots a_n$ 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 $H_n = H \otimes \ldots \otimes H$ be the application of H to each qubit of a row of n qubits. Show that

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

(c) (the Bernstein–Vazirani problem)
For each a consider the function f_a which is a balanced function if $a \neq 00 \ldots 0$ (as shown above). Show that the DJ algorithm will perfectly distinguish and identify the $2^n - 1$ balanced functions f_a (for $a \neq 00 \ldots 0$) 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.