QUANTUM INFORMATION

MFF UK

(0) The Toffoli gate $T : (a, b, c) \mapsto (a, b, c \oplus ab)$ is said to be able to *copy states*, i.e. $T : (a, 1, 0) \mapsto (a, 1, a)$. But we have already seen the *no-cloning theorem*, stating that no unitary operator U acting on, say 2-cubit system, can clone states, i.e. realize the mapping $|\varphi\rangle \otimes |0\rangle \mapsto |\varphi\rangle \otimes |\varphi\rangle$. Aren't these two statements contradictory?

(1) The natural analogy for the states $|+\rangle$ and $|-\rangle$ in a 2-cubit system are the so-called *Bell's states* defined as

$$|\beta_{xy}\rangle = \frac{|0y\rangle + (-1)^x |1\overline{y}\rangle}{\sqrt{2}},$$

where x, y are $0, 1$ and $\overline{y}$ is defined as $1 - y$.

Show that the four vectors $|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle$ form an orthonormal basis of $\mathbb{H}^2$. Express the circuit realizing $|xy\rangle \mapsto |\beta_{xy}\rangle$ as a composition of the single-cubit Hadamard operator H and the CNOT gate.

(2) (Quantum teleportation) Contrary to the no-cloning theorem, it is possible to *teleport* quantum states using just some classical communication channel. However, the teleported cubit is destroyed for it's original owner and so the no-cloning theorem is not contradicted.

The process can be described as follows: two parties (Alice and Bob) first create an entangled state $|\beta_{00}\rangle$ (prove that this state is, indeed, entangled) and share it between each other. This formally means that Alice is able to measure $|\beta_{00}\rangle$ (and any other 2-cubit state) on the first cubit (her measurement has the form $m_1 P_1 + m_2 P_2$, where P_1 is a projection operator onto the space generated by $|00\rangle$ and $|01\rangle$ and P_2 is a projection onto the space generated by $|10\rangle$ and $|11\rangle$). Similarly, Bob is able to measure the second cubit.

Alice is then given some arbitrary single-cubit state $|\varphi\rangle$ which she wants to teleport to Bob. For it she performs a CNOT operation on her pair of cubits (formally, she realizes the mapping $\mathrm{CNOT} \otimes id$ applied to $|\varphi\rangle \otimes |\beta_{00}\rangle$) followed by the Hadamard operator applied to the first cubit (again, we formally mean the operator $H \otimes id \otimes id$).

Finally, she measures both of her cubits separately and sends the results of her measurements via some classical communication channel to Bob. Depending upon the received data, Bob applies Pauli matrices Z and/or X to his single cubit. Recall that X realizes $|0\rangle \mapsto |1\rangle$ and $|1\rangle \mapsto |0\rangle$ and Z realizes $|0\rangle \mapsto |0\rangle$ and $|1\rangle \mapsto -|1\rangle$.

Finish the description of the protocol, draw it's diagram and verify that $|\varphi\rangle$ is indeed teleported to Bob and destroyed for Alice.

(3) Verify that applying

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$

to the first cubit in a 2-cubit system is equivalent to the controlled application of

$$\begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$

to the second cubit.

Also, verify the correctness of the circuit realizing controlled application of a single-cubit operator U from the lecture notes.

(4) Compute square roots of Pauli matrices X, Y, Z and the Hadamard matrix H.

(5) Express the operator acting on a 4-cubit system by applying Hadamard H gate to the fourth cubit controlled by the parity of the first 3 cubits as a combination of Toffoli gates and single-controlled single-cubit operators.

(6) Express the two-level operator M defined as

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & c & 0 & d \end{pmatrix}$$

as a composition of controlled single-cubit operators.

Express the two-level operator acting non-identically on $|0000\rangle$ and $|1111\rangle$ as a composition of controlled single-cubit operators.

(7) Decompose the matrix

$$\frac{\sqrt{3}}{3}\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 \\ 1 & -1 & 0 & 1 \\ 1 & 1 & -1 & 0 \end{pmatrix}$$

into composition of two-level operators.