33-658, 758 Quantum Computation and Information Spring Semester, 2014
Assignment No. 6. Due Tuesday, February 25

READING:

BLUM = "Classical Algorithms", lectures by Avrim Blum, Course web site
CLRS = Cormen, Leiserson, Rivest, and Stein, Introduction to Algorithms (Library reserve)
DPV = Dasgupta, Papadimitriou, and Vazirani. Algorithms (Library reserve)
MERMIN = N. D. Mermin, Quantum Computer Science (Library reserve)
PITTENGER = A. O. Pittenger, An Introduction to Quantum Computing Algorithms (Library reserve)
QCQI = Nielsen and Chuang, Quantum Computation and Quantum Information
QIT = "Quantum Information Types" Course web site
TELEPORT = "Dense Coding, Teleportation, No Cloning" Course web site

Types of quantum information: QIT. More details in Secs. I, II, and III of "Types of Quantum Information", Course web site.

Dense Coding: QCQI Sec. 2.3; TELEPORT; The original paper by Bennett and Wiesner, reference in QCQI p. 119, is also worth reading

No cloning: QCQI Sec. 12.1, and Proposition 12.18 in Sec. 12.6.3; TELEPORT

Teleportation: QCQI Secs. 1.3.7, 4.4; TELEPORT; Bennett et al., Phys. Rev. Lett. 70 (1993) 1895 (Original paper); If ambitious look at R. B. Griffiths, Phys. Rev. A 66 (2002) 012311.

Number-theoretic algorithms: CLRS Ch. 31; DPV Ch. 1; QCQI App. 4; BLUM

Complexity theory: CLRS Ch. 34; DPV Ch. 8; QCQI Ch. 3; BLUM

Public key cryptography (RSA): QCQI App. 5. A helpful summary of the associated number theory concepts will be found in QCQI App. 4. Stinson, *Cryptography: theory and practice*, Ch. 4.

READING AHEAD:

Deutsch-Jozsa algorithm: QCQI Sec. 1.4; PITTENGER Sec. 3.1

Shor factoring: QCQI Ch. 5 (not too easy); MERMIN Ch. 3; PITTENGER Secs. 3.4 to 3.7; E. Gerjuoy, Am. J. Phys. 73 (2005) 521

EXERCISES:

1. Turn in at most one page, and not less than half a page, indicating what you have read, examples or exercises (apart from those assigned below) that you worked out, difficulties you encountered, questions that came to mind, etc. You may include complaints about the course.

1b. Only for students enrolled in 33-758: Summarize in half a page to a page what you learned from the most recent seminar, the one on February 11 (second seminar on Bell inequalities).

2. Dense coding is possible using a tensor product $\mathcal{H} = \mathcal{H}_a \otimes \mathcal{H}_b$ of two spaces of equal dimension $d = d_a = d_b$ when d is greater than 2. What is needed is a basis of $\mathcal{H}$ consisting of fully-entangled states with the property that it is possible to map any basis state to any other basis state using unitary operations on $\mathcal{H}_a$ alone, or on $\mathcal{H}_b$ alone. Construct such a basis for $d = 3$ in the following way, assuming that $\mathcal{H}_a$ (and likewise $\mathcal{H}_b$) is spanned by the three orthonormal states $|0\rangle$, $|1\rangle$, and $|2\rangle$.

a) Construct three fully entangled and mutually orthogonal states which are linear combinations of $|00\rangle$, $|11\rangle$ and $|22\rangle$. [Hint No. 1: $(|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}$ is fully entangled. Hint No. 2: What are the three cube roots of 1, and what is their sum?]

b) Repeat (a) with the three states $|01\rangle$, $|12\rangle$ and $|20\rangle$, and then with three other states, to arrive at nine states that form an orthonormal basis of $\mathcal{H}$.

c) What are the unitary operations on $\mathcal{H}_a$ which will map the nine basis states onto one another? You do not have to display a complete set of such unitaries if you make it plain from your discussion and examples that you could do so if necessary.

3. No cloning. (See the end of the "No Cloning" section of the notes "Dense Coding, Teleportation, No Cloning.") Show that if there is a collection of d linearly-independent states $\{|\phi^j\rangle\}$, $1 \le j \le d$, each of which is perfectly transmitted through a quantum channel in the sense that for a fixed unitary T and initial $|c\rangle$,

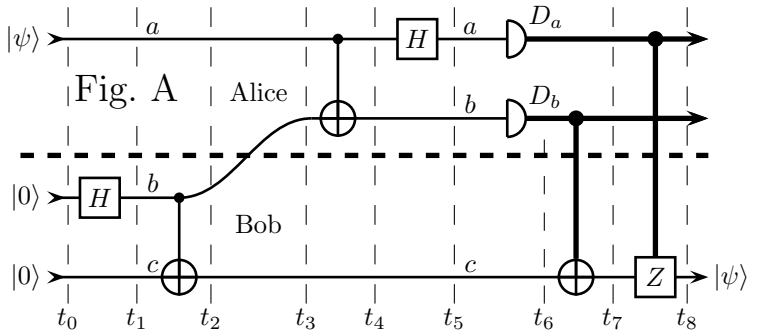
$$T\Big(|\phi^j\rangle \otimes |c\rangle\Big) = |\phi^j\rangle \otimes |c^j\rangle,$$

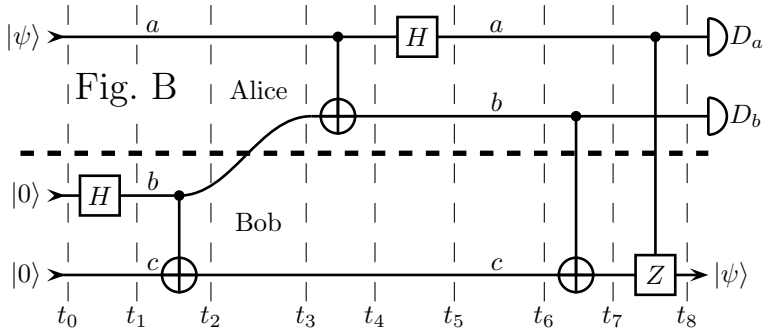
where the $\{|c^j\rangle\}$ are assumed to be normalized but not necessarily orthogonal to each other, then *provided* suitable nonorthogonality conditions are satisfied it is the case that all states in the subspace spanned by the $\{|\phi^j\rangle\}$ are also transmitted perfectly. What are these nonorthogonality conditions, and in particular is it necessary that each $|\phi^j\rangle$ be nonorthogonal to every other $|\phi^k\rangle$ with $k \neq j$, or is it possible to have $\langle\phi^j|\phi^k\rangle = 0$ for some pairs j, k? As part of the exercise, show that if the inner product of two normalized kets $|c'\rangle$ and $|c''\rangle$ is 1, the kets are identical. [Hint. What is the norm of $|c'\rangle - |c''\rangle$?]

4. Teleportation using measurements (A); quantized version (B).

a) Assume a general initial state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, and work out the unitary time development of the three qubits in Fig. B for $t \geq t_2$ starting with $|\Psi_2\rangle = |\psi\rangle \otimes (|00\rangle + |11\rangle)/\sqrt{2}$ at t_2. In particular obtain $|\Psi_5\rangle$ and $|\Psi_8\rangle$ at times t_5 and t_8.

b) If you have done (a) correctly, you will find that $|\Psi_8\rangle$ is a product of the form $|\omega\rangle\otimes|c\rangle$, where $|\omega\rangle$ and $|c\rangle$ are pure states on $\mathcal{H}_a \otimes \mathcal{H}_b$ and $\mathcal{H}_c$, respectively. Give an argument that it *must* be of this form if the c output of the channel is to always be the same as the a input. [Hint. What will happen if instead you have an entangled state, and measure the output to see if it is always the same as the input?] Also, how can you see from $|\Psi_8\rangle$ that the outcomes of D_a and D_b provide no information about $|\psi\rangle$?





c) Show that at time t_6 in Fig. B the information about $|\psi\rangle$ is contained in qubits a and b in the sense that it could be recovered from them without access to c by modifying the circuit at later times. (This is in contrast with the situation at t_6 in the circuit in Fig. A, where information about $|\psi\rangle$ is *not* present in the classical bits representing the measurement outcomes.)

5. a) Suppose the classical bit needed to apply the final Z gate in the preceding problem is lost, so the Z gate is never activated. This corresponds to omitting the final CZ gate in part B of the figure, so the situation at t_8 is the same as the situation at t_7. What can you say about the resulting channel from qubit a at t_0 to the final qubit c (at time t_7)? In particular, what happens to the X, Y, and Z types of information at the channel entrance?

b) Now address the same question supposing that it is the other classical bit that is lost, so that the NOT operation between t_6 and t_7 never occurs, but the final Z gate is carried out in accordance with the protocol.

6. a) List the elements of Z_{15}^* and check that there are $\varphi(15)$ of them, where $\varphi(n) = \prod_{j=1}^{k} p_j^{\alpha_j - 1}(p_j - 1)$ for $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ the prime factorization of n.

b) Find the order of each element of Z_{15}^*.

c) Find the multiplicative inverse of each element of Z_{15}^*.