Quantum Information and Computation
Homework 1

(Report Due: 23:30, March 15, 2022)

1. **(15 points) Basic entanglement for two qubits.**

   (a) **(5 points)** Show that the state $|A_k\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + (-1)^k|11\rangle)$ is entangled if $k = 1$ and unentangled if $k = 0$. Express the latter explicitly as a product state.

   (b) **(5 points)** Can $|A_k\rangle$ for $k = 0$ or 1 be prepared from $|0\rangle|0\rangle$ by applying only 1-qubit gates (i.e. an 1-qubit unitary operation) on $|0\rangle|0\rangle$? Give a reason for your answer.

   (c) **(5 points)** Generalizing 1a, show that $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$ is entangled if and only if $\alpha\delta - \beta\gamma \neq 0$.

2. **(10 points) Born rule, Pauli operations.**
   Let $|\psi\rangle = a|0\rangle + b|1\rangle$ be any 1-qubit quantum state. Suppose we receive one of the four states $|\psi\rangle$, $X|\psi\rangle$, $Y|\psi\rangle$, and $Z|\psi\rangle$, with equal prior probabilities of $\frac{1}{4}$. (The action on $|\psi\rangle$ is called Pauli-twirling.)

   Show that any outcome of any projective measurement on the Pauli-twirled version of $|\psi\rangle$ has probability half.

   Remark. Hence, the received state contains no information at all about the identity of $|\psi\rangle$. Namely, in the quantum teleportation protocol, without the two bits information from Alice (after she performs the local operations), Bob does not learn anything about the teleportated state from his system.

3. **(25 points) Schmidt form; making 2-qubit states**
   The *Schmidt decomposition* theorem for bipartite quantum states is the following:

   Theorem. *Let $|\psi\rangle_{AB}$ be any quantum state of a composite system comprising an m dimensional system A and n dimensional system B. Let $d = \min\{m, n\}$.*
   Then there are orthonormal bases $\{|\alpha_1\rangle, \ldots, |\alpha_m\rangle\}$ of A and $\{|\beta_1\rangle, \ldots, |\beta_n\rangle\}$ of B (called Schmidt bases *for $|\psi\rangle$) and non-negative real numbers $\lambda_1, \ldots, \lambda_d$ (called the* Schmidt coefficients *of $|\psi\rangle$), such that*

   $$|\psi\rangle = \sum_{i=1}^{d} \lambda_i |\alpha_i\rangle |\beta_i\rangle,$$

   i.e. when expressed in the Schmidt bases, $|\psi\rangle$ has no cross terms $|\alpha_i\rangle|\beta_j\rangle$ for $i \neq j$.
   The number of non-zero Schmidt coefficients is called the Schmidt rank *of $|\psi\rangle$.*

   We will consider the Schmidt decomposition of states of two qubits (i.e. $m = n = 2$).

(a) (**5 points**) By inspection (or otherwise) find Schmidt bases, coefficients and ranks for the product state $|a\rangle|b\rangle$ and for $|A_1\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$.
Show that $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle+|{-}{-}\rangle)$ and deduce that Schmidt bases are not uniquely determined if two Schmidt coefficients are equal.

(b) (**10 points**) Recall the statement of the singular value decomposition theorem for matrices (you may google it or find it in standard Textbooks if you don't know it). Here we will use it for 2×2 matrices. Writing a general 2-qubit state as $|\psi\rangle = \sum_{ij} a_{ij}|ij\rangle$, use the singular value decomposition theorem to prove Schmidt decomposition theorem for pairs of qubits.
(Note that the Schmidt form for higher dimensions follows similarly from the singular value decomposition theorem for larger matrices.)

(c) (**10 points**) Let $\{|\alpha_0\rangle = a|0\rangle + b|1\rangle, |\alpha_1\rangle = c|0\rangle + d|1\rangle\}$ 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 $U|1\rangle = |\alpha_1\rangle$.
Hence or otherwise, show that any 2-qubit state can be manufactured from $|0\rangle|0\rangle$ by application of a sequence of unitary gates comprising only 1-qubit gates and at most just a *single* application of the 2-qubit $CNOT$ gate. For which states is the $CNOT$ gate not required?

(d) (**Bonus 5 points**) The Schmidt form does *not* in fact generalize to *tri*-partite systems. To see this, show that there are states $|\psi\rangle_{ABC}$ of three qubits that cannot be expressed as

$$|\psi\rangle = \sum_{i=1}^{2} \lambda_i |\alpha_i\rangle|\beta_i\rangle|\gamma_i\rangle$$

(i.e. with no cross terms in the bases) for any triple of bases $\{|\alpha_i\rangle\}, \{|\beta_i\rangle\}, \{|\gamma_i\rangle\}$. You may assume that Schmidt bases are unique (up to overall phases and ordering of vectors) if the Schmidt coefficients are different. It may be helpful to begin with the (valid) Schmidt form of $|\psi\rangle_{ABC}$ for the *bi*-partition of A vs. BC.

4. (**20 points**) **No-deleting principle.**
A *deleting operation* for two distinct non-orthogonal states $|\psi_i\rangle$ with $i \in \{0,1\}$ is any process acting on two copies $|\psi_i\rangle|\psi_i\rangle$ with an ancilla $|M\rangle$, effecting the following:

$$|\psi_i\rangle|\psi_i\rangle|M\rangle \mapsto |\psi_i\rangle|0\rangle|M_i\rangle$$

i.e. given two copies we 'delete' one of them. Here $|0\rangle$ is any fixed state (independent of i) and $|M_i\rangle$ is a state that can depend on i.

(a) (**10 points**) Show that if such a deleting operation is unitary then $|\psi_i\rangle$ can always be reconstituted from $|M_i\rangle$ alone i.e there is a unitary operation U with $U|0\rangle|M_i\rangle = |\psi_i\rangle|N\rangle$ where $|N\rangle$ is independent of i. In this sense, quantum information cannot be deleted by a unitary process, even if we are given a second copy to help delete it; it can only be moved out to 'another place' ("the rubbish bin") from where it can always be perfectly retrieved.

(b) (**5 points**) Show that quantum information can be deleted if we allow measurements in the process.

(c) (**5 points**) Can *classical* information be deleted by purely reversible Boolean operations (given, as above, an ancilla to help)?

5. (**15 points**) **Unambiguous discrimination.**
Let $\{|\alpha_1\rangle, \dots, |\alpha_n\rangle\}$ be a set of n quantum states. They can be unambiguously discriminated if there is a quantum process and a measurement with $n+1$ outcomes labeled $1, \dots, n$ and 'fail' such that if the outcome k occurs then the input state was certainly $|\alpha_k\rangle$, and if outcome 'fail' occurs then the process was inconclusive. Also for every k, on input $|\alpha_k\rangle$, outcome k must have a *non-zero* probability of occurring.

You may assume that any prospective discrimination process is a unitary process (with inclusions of ancillas) having just a final measurement at the end. (This is called the *Deferred Measruement Principle*; see e.g. [§4.4, N&C].)

(a) (**15 points**) Show that if the states can be unambiguously discriminated then they must form a linearly independent set.

(b) (**Bonus 5 points**) Show that if the states are linearly independent then they can be unambiguously discriminated. (It may help to begin by adjoining an n-dimensional ancilla.)

6. (**15 points**) **Ambiguous discrimination.** Alice sends Bob one of N equally likely states $|\alpha_k\rangle$ for $k = 1, \dots, N$, each being a state in d dimensions, representing the message k. On receiving the state Bob attempts to read Alice's message by first adjoining an ancilla $|A\rangle$ to the received state and then performing a measurement on the total state, with projection operators Π_k, $k = 1, \dots, N$ respectively for concluding that the message was k.

(a) (**15 points**) Write down an expression for the probability P_S that Bob will correctly identify Alice's intended message k.

(b) (**10 points**) Show that for any measurement we have $P_S \le d/N$.
Hint: Some results in Homework 0 maybe useful. For example, if X is positive semi-definite and Π is a projection then $\Pi X \Pi$ is positive semi-definite. Here you may treat Π as projection onto the span of the N states $|\alpha_k\rangle |A\rangle$ in the enlarged space with the ancilla. If you can show that this subspace has dimension at most d, then the projection has trace at most d. Other useful facts might include that if X is positive semi-definite then $\langle\psi| X |\psi\rangle \le \mathrm{Tr}[X]$ for any normalized state vector $|\psi\rangle$.

(c) (**5 points**) Is the bound d/N on P_S here tight for a given set of N states $|\alpha_k\rangle$ in d dimensions? Give a reason for your answer.

Remark. Thus we see that d-dimensional states can never be used to reliably send more than d messages, and if we attempt to use larger N's then the success probability will be correspondingly necessarily worse. This proves the resource inequality: 1 qubit $\not\geq N$ cbits $\forall N > 1$.