January 27, 2020

1. No communication (/25).

Quantum mechanics is a local theory, in the sense that not even entanglement can be used to communicate information faster than light. However, this is not quite immediate but is a theorem that has to be proved. (a) Consider a state $|\psi\rangle = \sum_{i,j=1}^{n} a_{i,j} |i\rangle |j\rangle$ which involves two registers (possibly entangled with each other). Explain why no operation that we perform on the first register only (including unitaries and measurements), can affect the probability of any outcome of a standard-basis measurement on the second register only. [Hint: Write out the $a_{ij}$’s as an $n \times n$ matrix. What is the effect of an operation on the first register only?] (b) Show that unitary operations on separate subsystems commute with each other: that is, $(U \otimes I)(I \otimes V) = (I \otimes V)(U \otimes I)$ for all U,V. (c) Combining parts a. and b. conclude that no unitary transformation or measurement performed on the first register only, can affect the outcome of an experiment on the second register only.
2. Conjugating CNOT (/25).

Show that if you apply Hadamard gates to qubits A and B, followed by a CNOT gate from A to B, followed by Hadamard gates to A and B again, the end result is the same as if you had applied a CNOT gate from B to A. [Note: The CNOT gate won’t be defined until the second lecture, so this problem is intended for after that.] The above illustrates a principle of quantum mechanics you may have heard about: that any physical interaction by which A influences B can also cause B to influence A (so for example, it is impossible to measure a particle’s state without affecting it).


Show that if \( u, v, w, z \) are real vectors then the inner product
\[
\langle |u \oplus v\rangle, |w \oplus z\rangle \rangle
\]
is equal to the product of inner products \( \langle u|w \rangle \cdot \langle v|z \rangle \).


1. How many functions \( f : \{0, 1, \cdots, q\}^n \rightarrow \{0, 1, \cdots, q\} \) are there?

2. How many \( n \)-length palindromic bit-strings are there?

3. How many one-to-one functions are there from a set with \( m \) elements to a set with \( n \) elements? (A function \( f \) is one to one if no two elements in the domain of \( f \) correspond to the same element in the range of \( f \).)