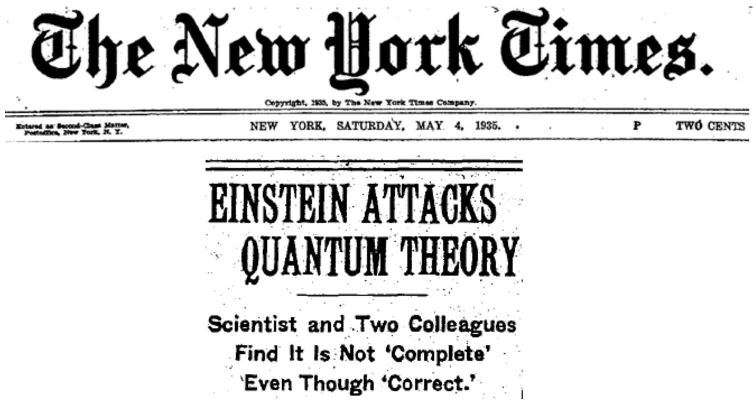
MATH 1800: Quantum Information Theory with Applications to Cryptography

# Entaglement and EPR pairs


The New York Times.

Copyright, 1935, by The New York Times Company.

NEW YORK, SATURDAY, MAY 4, 1935. P TWO CENTS

EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

**Problem 1.** (20 pts) For each of the vectors $\mathcal{S}$ below either write its decomposition in a tensor product of two vectors or show that it is indecomposable.

(a) $\mathcal{S} = 2e_1 \otimes e_2 - e_1 \otimes e_1 \in \mathbb{C}^2 \otimes \mathbb{C}^2$

(b) $\mathcal{S} = e_1 \otimes e_1 - e_1 \otimes e_2 - e_2 \otimes e_1 + e_2 \otimes e_2 \in \mathbb{C}^2 \otimes \mathbb{C}^2$

(c) $\mathcal{S} = e_1 \otimes e_2 - e_2 \otimes e_1 \in \mathbb{C}^2 \otimes \mathbb{C}^2$

**Problem 2.** (15 pts) Do indecomposable vectors form a vector subspace inside $V \otimes W$? If 'yes' give a proof, if 'no', give an example of two vector spaces $V, W$ and two indecomposable vectors $\mathcal{S}_1, \mathcal{S}_2 \in V \otimes W$ with $\mathcal{S}_1 + \mathcal{S}_2$ not indecomposable.

**Problem 3.** (15 pts) Consider the Greenberger-Horne-Zeilinger state $\mathsf{GHZ}_n = \frac{1}{\sqrt{2}}(|\underbrace{00\ldots0}_{n}\rangle + |\underbrace{11\ldots1}_{n}\rangle)$ and construct a quantum circuit for the gate $|\underbrace{00\ldots0}_{n}\rangle \to \mathsf{GHZ}_n$ using Hadamard and $\underbrace{\mathsf{C}\ldots\mathsf{C}}_{k}\mathsf{NOT}$ gates with $1 \le k \le n-1$. No ancilla qubits are allowed.

(a) $n = 2$.

(b) $n = 3$.

(c) Any $n \in \mathbb{Z}_{>1}$.

**Problem 4.** (20 pts) Suppose Alice and Bob share an EPR-pair, $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Then they can transmit two classical bits by sending one qubit over the channel; the procedure is called *superdense coding*. This exercise will show how this works.

(a) Alice has classical bits $a$ and $b$. Suppose she applies an $X = \mathrm{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$-gate on her half of the EPR-pair if $a = 1$, followed by a $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$-gate if $b = 1$ (she does both if $(a, b) = (1, 1)$, and neither if $(a, b) = (0, 0)$). Write the resulting 2-qubit state for the four different pairs of bits $(a, b)$.

(b) Suppose Alice sends her half of the state to Bob, who now has two qubits. Show that Bob can determine both $a$ and $b$ from his state, using Hadamard and $\mathrm{CNOT}$ gates, followed by a measurement in the standard basis.

**Remark.** You have just established another **Bennet's law**[1]: 1 ebit + 1 qubit $\geq$ 2 classical bits.

**Problem 5.** (30 pts) Let $U_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$ be the operator of rotation by an angle $\theta$ with $|\varphi\rangle = U_\theta(|0\rangle)$ and $|\varphi^\perp\rangle = U_\theta(|1\rangle)$.

(a) Show that $ZX(|\varphi^\perp\rangle) = |\varphi\rangle$.

[1] In agricultural economics and development economics, Bennett's law observes that as incomes rise, people eat relatively fewer calorie-dense starchy staple foods and relatively more nutrient-dense meats, oils, sweeteners, fruits, and vegetables. Bennett's law is related to Engel's law, which considers the relationship between rising household incomes and total food spending 🙂

(b) Show that an EPR-pair, $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, can also be written as $|\psi\rangle = \frac{1}{\sqrt{2}}(|\varphi\varphi\rangle + |\varphi^{\perp}\varphi^{\perp}\rangle)$. [2]

(c) Suppose Alice and Bob start with an EPR-pair. Alice applies $U_\theta^{-1}$ to her qubit and then measures it in the standard basis. What state does Bob have if her outcome was $|0\rangle$, and what state does he have if her outcome was $|1\rangle$?

(d) Suppose Alice knows the angle of rotation $\theta$ (can apply $U_\theta$ and $U_\theta^{-1}$) but Bob does not. Give a protocol (algorithm) that uses one EPR-pair and one classical bit of communication where Bob ends up with the qubit $|\varphi\rangle$ (in contrast to general teleportation of an unknown qubit, which uses 1 EPR-pair and 2 bits of communication).

[2] **Hint:** you need to check that $U_\theta e_1 \otimes U_\theta e_1 + U_\theta e_2 \otimes U_\theta e_2 = e_1 \otimes e_1 + e_2 \otimes e_2$, where $e_1 = (1,0)$ and $e_2 = (0,1)$ form the standard basis of $\mathbb{C}^2$.