Solutions to Daily Due Nov 2 (AI generated)

Math 4440/5440, Coding and Cryptography, Fall 2026

Generated by Claude for Katherine E. Stange
(all computations computer-verified)

Problem 1: $\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$

The outcomes 01 and 10 each have probability $\frac{1}{2}$; the outcomes 00 and 11 have probability 0.

1. $\Pr(\text{first bit} = 0) = \Pr(00) + \Pr(01) = 0 + \frac{1}{2} = \frac{1}{2}$.
2. $\Pr(\text{second bit} = 0) = \Pr(00) + \Pr(10) = 0 + \frac{1}{2} = \frac{1}{2}$.
3. $\Pr(00) = 0$. Each bit alone is a fair coin, but they are never both 0: the bits always disagree. (So this state is entangled, like the Bell state but with the bits anti-correlated.)

Problem 2: entangled or not?

A state is *not* entangled if it factors as a product of single-qubit states. Factoring is the way to show "not entangled"; a contradiction in the coefficients is the way to show "entangled".

1. $|111\rangle = |1\rangle|1\rangle|1\rangle$. **Not entangled.**
2. $\frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle = |1\rangle\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$. **Not entangled.**
3. $\frac{1}{\sqrt{2}}|110\rangle + \frac{1}{\sqrt{2}}|111\rangle = |1\rangle|1\rangle\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$. **Not entangled.**
4. $\frac{1}{\sqrt{2}}|010\rangle + \frac{1}{\sqrt{2}}|111\rangle$. **Entangled.** The middle qubit does factor out: the state is $|1\rangle$ in the middle slot, times $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ on the outer two qubits. But that outer state is the Bell state, which we showed is not a product (daily due Oct 30, problem 3(4)). Directly: a product $(x_0|0\rangle + x_1|1\rangle)(y_0|0\rangle + y_1|1\rangle)(z_0|0\rangle + z_1|1\rangle)$ would need $x_0y_1z_0 \neq 0$ (coefficient of $|010\rangle$) and $x_1y_1z_1 \neq 0$ (coefficient of $|111\rangle$), so all of x_0, x_1, y_1, z_0, z_1 are nonzero; but then the coefficient of $|011\rangle$, namely $x_0y_1z_1$, would be nonzero too, whereas it is 0.

Problem 3: measuring one qubit of $\frac{1}{\sqrt{2}}|010\rangle + \frac{1}{\sqrt{2}}|111\rangle$

Add up the probabilities ($\frac{1}{2}$ each for 010 and 111) of the outcomes with a 0 in the given position:

- **First qubit:** 010 has first bit 0, 111 does not. $\Pr = \frac{1}{2}$.
- **Middle qubit:** both outcomes have middle bit 1. $\Pr = 0$.
- **Last qubit:** 010 has last bit 0, 111 does not. $\Pr = \frac{1}{2}$.

Problem 4: measuring the first qubit

Rule: group the terms by the value of the first qubit. The probability of each outcome is the total squared length of its group, and the post-measurement state is that group, renormalized.

(1) The Bell state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.

outcome bit	probability	outcome state
0	$\frac{1}{2}$	$\|00\rangle$
1	$\frac{1}{2}$	$\|11\rangle$

After the measurement, the second qubit is no longer in superposition: it is $|0\rangle$ or $|1\rangle$, matching the first.

(2) $\frac{1}{\sqrt{14}}|01\rangle + \frac{2i}{\sqrt{14}}|10\rangle + \frac{3}{\sqrt{14}}|11\rangle$. The first-bit-0 group is $\frac{1}{\sqrt{14}}|01\rangle$, with squared length $\frac{1}{14}$. The first-bit-1 group is $\frac{2i}{\sqrt{14}}|10\rangle + \frac{3}{\sqrt{14}}|11\rangle$, with squared length $\frac{4}{14} + \frac{9}{14} = \frac{13}{14}$. Renormalizing the second group means dividing by $\sqrt{13/14}$, i.e. multiplying by $\frac{\sqrt{14}}{\sqrt{13}}$:

outcome bit	probability	outcome state
0	$\frac{1}{14}$	$\|01\rangle$
1	$\frac{13}{14}$	$\frac{2i}{\sqrt{13}}\|10\rangle + \frac{3}{\sqrt{13}}\|11\rangle$

Check: $\left|\frac{2i}{\sqrt{13}}\right|^2 + \left|\frac{3}{\sqrt{13}}\right|^2 = \frac{4+9}{13} = 1$.

Problem 5: complex conjugates

$$\overline{3+7i} = 3-7i, \qquad \overline{8} = 8, \qquad \overline{8i} = -8i.$$

Conjugation flips the sign of the imaginary part; a real number is its own conjugate.

Problem 6: a conjugate transpose, and a unitarity check

Let $M = \begin{pmatrix} 1 & 2+i \\ 3i & i \end{pmatrix}$. Transpose, then conjugate every entry:

$$M^\dagger = \overline{M}^T = \begin{pmatrix} 1 & -3i \\ 2-i & -i \end{pmatrix}.$$

M is unitary if $M^\dagger M = I$. Compute:

$$M^\dagger M = \begin{pmatrix} 1 & -3i \\ 2-i & -i \end{pmatrix}\begin{pmatrix} 1 & 2+i \\ 3i & i \end{pmatrix} = \begin{pmatrix} 1+(-3i)(3i) & (2+i)+(-3i)(i) \\ (2-i)+(-i)(3i) & (2-i)(2+i)+(-i)(i) \end{pmatrix} = \begin{pmatrix} 10 & 5+i \\ 5-i & 6 \end{pmatrix}.$$

This is not the identity, so M is **not unitary**. (A quick way to see this without the full product: the first column of M is $(1, 3i)$, with squared length $1+9 = 10 \neq 1$. A unitary matrix's columns all have length 1, so a unitary matrix never stretches a state. Here $M|0\rangle$ has length $\sqrt{10}$.)

Problem 7: the Pauli Z gate

$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ leaves $|0\rangle$ alone and negates $|1\rangle$:

$$Z\left(\tfrac{1+2i}{\sqrt{6}}|0\rangle + \tfrac{1}{\sqrt{6}}|1\rangle\right) = \tfrac{1+2i}{\sqrt{6}}|0\rangle - \tfrac{1}{\sqrt{6}}|1\rangle.$$

Measuring in the $|0\rangle$, $|1\rangle$ basis: the input gives 0 with probability $\frac{|1+2i|^2}{6} = \frac{5}{6}$ and 1 with probability $\frac{1}{6}$; the output gives $\frac{|1+2i|^2}{6} = \frac{5}{6}$ and $\frac{|-1|^2}{6} = \frac{1}{6}$. **The same.** Z only changes a sign (a phase), and phases are invisible to measurement in this basis. They are not invisible in other bases, which is the point of the next problem.

Problem 8: $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ versus $|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

(1) Both states have coefficients of squared length $\frac{1}{2}, \frac{1}{2}$, so measuring either in the $|0\rangle$, $|1\rangle$ basis gives 0 or 1 with probability $\frac{1}{2}$ each. The two states produce identical statistics, so no number of such measurements can tell them apart. (Also, you only get to measure a given photon once.) The difference between them is a relative sign, which this measurement can't see.

(2) With $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$:

$$H|\psi\rangle = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \tfrac{1}{2}\begin{pmatrix} 2 \\ 0 \end{pmatrix} = |0\rangle, \qquad H|\phi\rangle = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \tfrac{1}{2}\begin{pmatrix} 0 \\ 2 \end{pmatrix} = |1\rangle.$$

Now measuring in the $|0\rangle$, $|1\rangle$ basis gives 0 with certainty for $H|\psi\rangle$ and 1 with certainty for $H|\phi\rangle$. **Yes**, one measurement now distinguishes them perfectly. Applying H and then measuring in the standard basis is the same as measuring in the basis $\{|\psi\rangle, |\phi\rangle\}$ (the V basis, in the photon language); the gate converts a sign difference into a difference the detector can see.

Problem 9: a gate sending $|0\rangle$ to $\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$

The first column of a matrix is where it sends $|0\rangle$, so the first column must be $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}$. For the matrix to be unitary, the second column must be a unit vector orthogonal to the first (using the complex inner product, which conjugates the first vector). One choice is $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}$: the inner product is $\frac{1}{2}\left(\overline{1}\cdot 1 + \overline{i}\cdot(-i)\right) = \frac{1}{2}\left(1 + (-i)(-i)\right) = \frac{1}{2}(1-1) = 0$. So

$$U = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$$

works: $U^\dagger U = \frac{1}{2}\begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = I$. This U is the Hadamard gate followed by the phase gate $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, i.e. $U = SH$. Many other answers work: the second column can be multiplied by any phase $e^{i\theta}$, and the second column can be any unit vector orthogonal to the first.