MASSACHUSETTS INSTITUTE OF TECHNOLOGY
Department of Physics, EECS, and Department of Applied Math

6.443J/8.371J/18.409/MAS.865 Spring 2006

Quantum Information Science

Problem Set #1 Solutions
(due 16-Feb-06)

Problem 1: (Review)

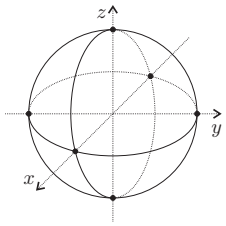
(a) The Pauli matrices

$$\sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

have eigenvalues ± 1. The corresponding eigenvectors are

$$|z+\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |x+\rangle = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad |y+\rangle = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix},$$
$$|z-\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad |x-\rangle = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}, \quad |y-\rangle = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \end{bmatrix}.$$

The density matrix of a single qubit can be expressed as $(1+\vec{n}\cdot\vec{\sigma})/2$ with $|\vec{n}| \leq 1$. We can plot $\vec{n}$ on a Bloch sphere. The eigenvectors of the Pauli matrices correspond to $\vec{n} = [\pm 1, 0, 0], [0, \pm 1, 0]$ and $[0, 0, \pm 1]$, respectively.



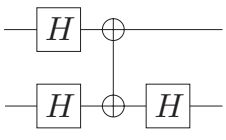
(b) The action of a CNOT on $\rho = \sum c_{jk} |j\rangle \langle k|$ is

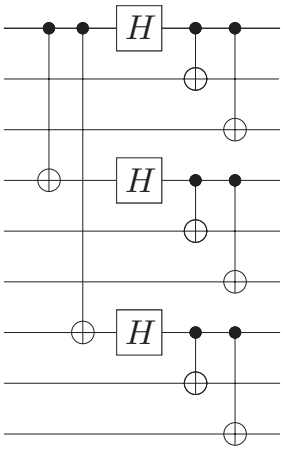
$$\begin{array}{llll} c_{00,00} \to c_{00,00}, & c_{00,01} \to c_{00,01}, & c_{00,10} \to c_{01,11}, & c_{00,11} \to c_{00,10}, \\ c_{01,00} \to c_{01,00}, & c_{01,01} \to c_{01,01}, & c_{01,10} \to c_{01,11}, & c_{01,11} \to c_{01,10}, \\ c_{10,00} \to c_{11,00}, & c_{10,01} \to c_{11,01}, & c_{10,10} \to c_{11,11}, & c_{10,11} \to c_{11,10}, \\ c_{11,00} \to c_{10,00}, & c_{11,01} \to c_{10,01}, & c_{11,10} \to c_{10,11}, & c_{11,11} \to c_{10,10}. \end{array}$$

It looks much simpler when we realize we can write it as $\rho \to U \rho U^\dagger$ with

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

(c) This circuit produces $(|00\rangle + |11\rangle)/\sqrt{2}$ from $|00\rangle$ using only C-PHASE and Hadamards.





(d) The encoding circuit for Shor's 9-qubit code is depicted above.

(e) Take the matrix for CNOT from (b), write out matrices

$$X_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad Z_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}, \tag{1}$$
$$X_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad Z_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix},$$

do a little algebra, and obtain

$$UX_1U = X_1X_2, \quad UX_2U = X_2, \quad UZ_1U = Z_1, \quad UZ_2U = Z_1Z_2.$$

(f) Let us rewrite $R_y(\theta) = \mathbb{I}\cos\frac{\theta}{2} - iY\sin\frac{\theta}{2}$ and $R_X(\theta) = \mathbb{I}\cos\frac{\theta}{2} - iX\sin\frac{\theta}{2}$. A rotation about the z-axis can be constructed by rotating by $\pi/2$ about x, rotating by θ about y, and then rotating back $\pi/2$ about x. Alternatively,

$$\begin{aligned} R_X(-\pi)R_Y(\theta)R_X(\pi) &= \frac{1}{\sqrt{2}}(\mathbb{I} + iX)\left(\mathbb{I}\cos\frac{\theta}{2} - iY\sin\frac{\theta}{2}\right)\frac{1}{\sqrt{2}}(\mathbb{I} - iX) \\ &= \mathbb{I}\cos\frac{\theta}{2} - i\frac{1}{2}(\mathbb{I} - iX)Y(\mathbb{I} + iX)\sin\frac{\theta}{2} = R_z(\theta), \end{aligned}$$

recalling that $[X, Y] = 2iZ$.

Problem 2: (Open Systems and the Operator Sum Representation)

(a) Let $\{E_j\}$ be the set of operation elements for $\mathcal{E}$ and $W_{jk} = \mathrm{tr}\left(E_j^\dagger E_k\right)$. It is straighforward to see that W_{jk} is hermitian. Write

$$\left(W^\dagger\right)_{jk} = W_{kj}^* = \mathrm{tr}\left(E_k^\dagger E_j\right)^* = \mathrm{tr}\left(E_k^T E_j^*\right) = \mathrm{tr}\left((E_k^T E_j^*)^T\right) = \mathrm{tr}\left(E_j^\dagger E_k\right) = (W)_{jk}\,.$$

Let us now look at the rows of the matrix W:

$$W = \begin{bmatrix} \mathrm{tr}\left(E_1^\dagger E_1\right) & \mathrm{tr}\left(E_1^\dagger E_2\right) & \dots & \mathrm{tr}\left(E_1^\dagger E_m\right) \\ \mathrm{tr}\left(E_2^\dagger E_1\right) & \mathrm{tr}\left(E_2^\dagger E_2\right) & \dots & \mathrm{tr}\left(E_2^\dagger E_m\right) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{tr}\left(E_{d^2+1}^\dagger E_1\right) & \mathrm{tr}\left(E_{d^2+1}^\dagger E_2\right) & \dots & \mathrm{tr}\left(E_{d^2+1}^\dagger E_m\right) \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix}.$$

The basis for the space of complex $d \times d$ matrices has d^2 elements. Therefore there can be only d^2 linearly independent matrices E_k. Let us reorder the matrices $\{E_k\}$ in such a way that the linearly independent ones come first. After this, we are assured that $E_a = \sum_{b=1}^{d^2} c_{ab} E_b$ for all $a > d^2$. Using the additivity of the trace, we see that all of the rows of W below d^2 are then linearly dependent on the rows above them. Therefore the rank of W is at most d^2.

Because W is Hermitian with rank at most d^2, there is a unitary matrix u that transforms W into a diagonal matrix $uWu^\dagger$ with at most d^2 nonzero entries. We can rewrite the elements of the matrix $uWu^\dagger$ as

$$w_i \delta_{ij} = \left(uWu^\dagger\right)_{ij} = u_{ia}\mathrm{tr}\left(E_a^\dagger E_b\right) u_{jb}^* = \mathrm{tr}\left(\left(u_{ia}^* E_a\right)^\dagger \left(u_{jb}^* E_b\right)\right).$$

This suggests that maybe we could use $u_{jb}^* E_b$ as the new operation elements. Let us then define a new set of at most d^2 operation elements

$$F_j = u_{jb}^* E_b.$$

Let us check and see that they equivalently express our original quantum operation:

$$\begin{aligned} \sum_j F_j \rho F_j^\dagger &= \sum_j \sum_{b,c} \left(u_{jb}^* E_b\right) \rho \left(u_{jc} E_c^\dagger\right) = \sum_{b,c} \left(u^\dagger u\right)_{bc} \left(E_b \rho E_c^\dagger\right) \\ &= \sum_{b,c} \delta_{bc} \left(E_b \rho E_c^\dagger\right) = \sum_b E_b \rho E_b^\dagger = \mathcal{E}(\rho). \end{aligned}$$

(b) We have two sets of operation elements:

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{bmatrix}, \qquad E_1 = \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{bmatrix},$$

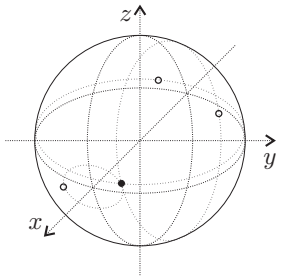
and

$$\tilde{E}_0 = \sqrt{\alpha} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \tilde{E}_1 = \sqrt{1-\alpha} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

where $\alpha = (1+\sqrt{1-\lambda})/2$. It is straightforward to check that both operations have the same action on a general ρ. Let us then just give the transformation $E_k = u_{kl}\tilde{E}_l$, obtained by simple algebra, using $\lambda = 4a(1-a)$.

$$u = \begin{bmatrix} \sqrt{\alpha} & \sqrt{1-\alpha} \\ \sqrt{1-\alpha} & -\sqrt{\alpha} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} \sqrt{1+\sqrt{1-\lambda}} & \sqrt{1-\sqrt{1-\lambda}} \\ \sqrt{1-\sqrt{1-\lambda}} & -\sqrt{1+\sqrt{1-\lambda}} \end{bmatrix}.$$

(c) We are looking for a quantum operation that outputs the completely mixed state $\mathbb{I}/2$, no matter what the input state ρ was. It takes the Bloch sphere as an input and shrinks it onto its center. We know from (a) that only four operation elements are needed. It turns out that this operation can be composed from simple rotations. Start with any point $\vec{n}_1$ on the Bloch sphere and rotate it by π about one of the axes, obtaining $\vec{n}_{2,3,4}$. The sum of these four vectors is zero, so we arrive at $\mathbb{I}/2$ no matter what the starting point was. This is a graphic interpretation of the quantum operation



$$\mathcal{E}(\rho) = \frac{1}{4}(\mathbb{I}\rho\mathbb{I} + X\rho X + Y\rho Y + Z\rho Z) = \mathbb{I}/2$$

with operation elements $E_k = \frac{1}{4}\sigma_k$. This operation can be also viewed as a simple one-time pad encryption of a single qubit. One can choose to employ one of the four operations $\{\mathbb{I}, X, Y, Z\}$ with equal probability. An eavesdropper would then see an encoded state $\mathcal{E}(\rho) = \mathbb{I}/2$, which does not hold any information about the encrypted input state ρ.

Problem 3: (Two-bit Amplitude Damping Code)

(a) For an input state $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ we have

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}, \quad E_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}, \quad \rho = \mathcal{E}\left(|\psi\rangle\langle\psi|\right) = \begin{bmatrix} a^2 & ab \\ ab & b^2 \end{bmatrix},$$

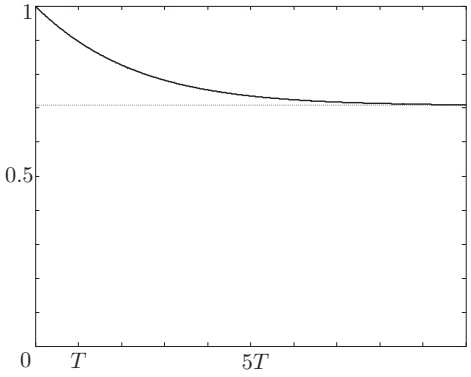
to make things simpler, we take a and b to be real. The fidelity of ρ state with respect to ψ is

$$F\left(|\psi\rangle, \rho\right) = \sqrt{\langle\psi|\,\rho\,|\psi\rangle} \;\; = \;\; \sqrt{a^4 + a^2b^2\left(\gamma + 2\sqrt{1-\gamma}\right) + b^4(1-\gamma)}.$$

Specifically for $|\psi_1\rangle = \left(|0\rangle + |1\rangle\right)/\sqrt{2}$,

$$F\left(|\psi_1\rangle, \rho_1\right) = \frac{1}{\sqrt{2}}\sqrt{1+\sqrt{1-\gamma}}.$$

We plot this as a function of time for $\gamma = 1-e^{-\frac{t}{T}}$. It asymptotically aproaches $1/\sqrt{2}$.

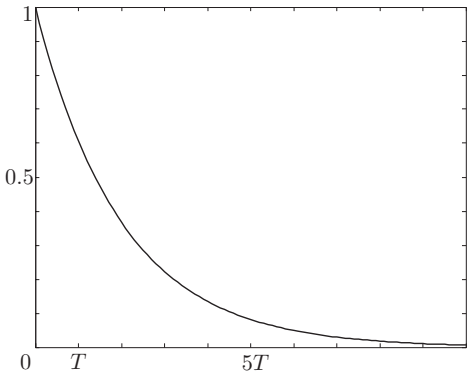


(b) When we rewrite F using $x = a^2 = 1 - b^2$, we obtain

$$F(x) = \sqrt{2x^2\left(1-\gamma-\sqrt{1-\gamma}\right) + x\left(3\gamma - 2 + 2\sqrt{1-\gamma}\right) + (1-\gamma)}.$$

For $0 \leq \gamma \leq 1$ and $0 \leq x \leq 1$ this is an increasing function, which gives the expected result that the state with $x = 0$, i.e. $|\psi_2\rangle = |1\rangle$ has the lowest fidelity at all times for the amplitude damping channel. The lower bound on fidelity at all times (take $x = 0$) is then

$$F_{min}(t) = \sqrt{1-\gamma} = e^{-\frac{t}{2T}}.$$



(c) Let us now use two qubit input states with $|\psi\rangle = a\,|01\rangle + b\,|10\rangle$. The output of the amplitude damping channel on this two-qubit state is

$$\begin{aligned}\rho' \;\; &= \;\; \mathcal{E}(|\psi\rangle) = \sum_{j,k=\{0,1\}} \left(E_j \otimes E_k\right)\,|\psi\rangle\,\langle\psi|\,\left(E_j \otimes E_k\right)^\dagger \\ &= \;\; \begin{bmatrix} \gamma & 0 & 0 & 0 \\ 0 & (1-\gamma)a^2 & (1-\gamma)ab & 0 \\ 0 & (1-\gamma)ab & (1-\gamma)b^2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \gamma\,|00\rangle\,\langle 00| + (1-\gamma)\,|\psi\rangle\,\langle\psi|\,.\end{aligned}$$

(d) The fidelity of ρ' with respect to ψ is simply

$$F\left(\rho', |\psi\rangle\right) = \sqrt{1-\gamma} = e^{-\frac{t}{2T}},$$

which is the same result as we had in (b), and thus the same plot.

(e) If we project ρ' into the space orthogonal to $|00\rangle$, we obtain the original state $|\psi\rangle$! However, this comes with a cost, the probability of obtaining a successful projection onto the space OG to $|00\rangle$ is $(1-\gamma)$. This relates well to the meaning of fidelity, which for mixtures of orthogonal states $\rho = p_\alpha |\alpha\rangle \langle\alpha| + p_\beta |\beta\rangle \langle\beta|$ gives $F\left(\rho, |\beta\rangle\right) = \sqrt{p_\beta}$.

Problem 4: (CSS and the 7-qubit Steane Code)

(a) The 16 codewords are the columns of the matrix GJ_{15}, where J_{15} is a matrix with binary expressions for 0 to 15 as columns.

$$\begin{aligned} GJ_{15} &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}. \end{aligned}$$

(b) The way we constructed the codewords, it is clear that it is enough to check $HG = 0$ for $Hx = HGJ_{15} = 0$ to be true. The matrix H checks the parity of bits 4567, 2367 and 1357.

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

(c) We know that $H(x+e) = He$, because $Hx = 0$ for codewords x. When a single error occurs, the error e is a vector with one nonzero entry, thus He is a column

of H. Now H is a Hamming code check matrix, constructed in such a way that its columns h_k are binary representations for k, i.e. the fifth column of H is $h_5 = [1\,0\,1]^T$. Therefore $H(x+e) = He$ tells us which bit to flip to correct the error e.

(d) It is clear that the distance of the code is $d(C) \leq 3$, because the second and the last codeword have Hamming distance 3. If you flip the first three bits of a codeword, you can convince yourself that H doesn't "see" it. Nevertheless, the distance is $d(C) = 3$, because if you flip any two bits of a codeword, the check matrix H would detect it (no two columns of H are linearly dependent).

(e) Let us take the code $C^\perp$ with $G' = H^T$ and $H' = G^T$. This code encodes $k = 3$ bits into $n = 7$ bits. Its codewords are

$$\begin{aligned} G'J_7 &= \begin{bmatrix} 0&0&1\\ 0&1&0\\ 0&1&1\\ 1&0&0\\ 1&0&1\\ 1&1&0\\ 1&1&1 \end{bmatrix} \begin{bmatrix} 0&0&0&0&1&1&1&1\\ 0&0&1&1&0&0&1&1\\ 0&1&0&1&0&1&0&1 \end{bmatrix} \\ &= \begin{bmatrix} 0&1&0&1&0&1&0&1\\ 0&0&1&1&0&0&1&1\\ 0&1&1&0&0&1&1&0\\ 0&0&0&0&0&1&1&1\\ 0&1&0&1&1&0&1&0\\ 0&0&1&1&1&1&0&0\\ 0&1&1&0&1&0&0&1 \end{bmatrix}. \end{aligned}$$

All these can be found in the codebook for C. Another way to see that $C^\perp \in C$ is to realize checking the codewords y_k of $C^\perp$ with H gives zero, because $Hy_k = HG'e_k = HH^Te_k = 0$, because one can check that $HH^T = 0$.

(f) Every codeword $y_k \in C$ (a column vector) can be expressed as $y_k = Ge_k$, where e_k is the binary representation of k.

$$x \cdot y_k = x^T G e_k = (G^T x)^T e_k = \alpha^T e_k.$$

Recall that G^T is the check matrix for the code $C^\perp$. Therefore if $x \in C^\perp$, we have $\alpha = G^T x = 0$, so $x \cdot y_k = 0$ for any $y_k \in C$. Thus

$$\sum_{y \in C} (-1)^{x \cdot y} = \sum_{y \in C} 1 = |C|, \quad \text{for } x \in C^\perp.$$

On the other hand, if $x \notin C^\perp$, $\alpha = G^T x$ is nonzero, and the sum can be expressed as

$$\sum_{y\in C}(-1)^{x\cdot y} = \sum_{e_k\in\{0,1\}^n}(-1)^{\alpha^T e_k} = 0, \quad \text{for } x \notin C^\perp.$$

(g) The size of $C^\perp$ is 8. Using

$$|\psi(x)\rangle = \frac{1}{\sqrt{|C^\perp|}}\sum_{y\in C^\perp}|x+y\rangle\,,$$

and the codewords for C and $C^\perp$ we obtain

$$\begin{aligned}
|\psi(0000000)\rangle &= \frac{1}{\sqrt{8}}\left(\begin{array}{c}|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ +|0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\end{array}\right), \\
|\psi(1111111)\rangle &= \frac{1}{\sqrt{8}}\left(\begin{array}{c}|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\ +|1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle\end{array}\right).
\end{aligned}$$

(h) If a phase error e_2 occurs, $|x+y\rangle$ is mapped onto $(-1)^{(x+y)\cdot e_2}|x+y\rangle$. Next, after a bit error e_1 we obtain

$$|\psi_{\text{b+p err}}\rangle = \frac{1}{\sqrt{|C^\perp|}}\sum_{y\in C^\perp}(-1)^{(x+y)\cdot e_2}|x+y+e_1\rangle\,.$$

What would happen though, if the bit-flip error happened first? We would obtain

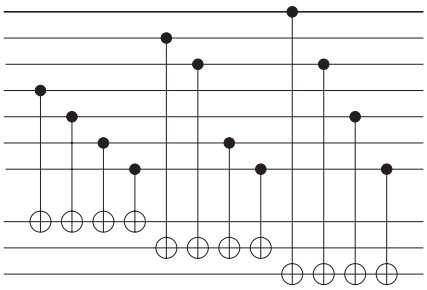
$$|x+y\rangle \quad \xrightarrow{e_1} \quad |x+y+e_1\rangle \quad \xrightarrow{e_2} \quad (-1)^{(x+y+e_1)\cdot e_2}|x+y+e_1\rangle\,.$$

This would give us

$$|\psi_{\text{p+b err}}\rangle = (-1)^{e_1\cdot e_2}\frac{1}{\sqrt{|C^\perp|}}\sum_{y\in C^\perp}(-1)^{(x+y)\cdot e_2}|x+y+e_1\rangle\,,$$

which is the previous result, just with an overall phase $\phi = (-1)^{e_1\cdot e_2}$. This is $+1$ for all bit-flips and phase-flips only, and it is -1 if both a bit-flip and a phase-flip occurred on a qubit, with the bit-flip coming first. This phase is obviously insignificant for logical qubits. However, can this overall -1 spoil things when we are computing on superpositions of encoded states, like $|0_L\rangle_1|1_L\rangle_2 - |1_L\rangle_1|0_L\rangle_2$ and an error occurs on the first qubit of the first encoded state? No, because both states $|0_L\rangle_1$ and $|1_L\rangle_1$ will acquire the extra phase ϕ, because the phase does not depend on x or y in the codewords, but rather only on the error that occurred. Therefore this overall ± 1 does not matter, and we can freely write

$$|\psi_{\text{b+p err}}\rangle = \frac{1}{\sqrt{|C^\perp|}}\sum_{y\in C^\perp}(-1)^{(x+y)\cdot e_2}|x+y+e_1\rangle\,.$$



(i) This is how you compute $|x\rangle|000\rangle \to |x\rangle|Hx\rangle$. From (c) we see that $|Hx\rangle$ is the bit representation of the flipped bit. We can now measure $|Hx\rangle$ to obtain e_1 and flip the errorneous bit back to get

$$|\psi_{\text{p err}}\rangle = \frac{1}{\sqrt{|C^{\perp}|}} \sum_{y \in C^{\perp}} (-1)^{(x+y)\cdot e_2} |x+y\rangle .$$

(j) Applying Hadamards to each qubit of

$$|\psi_{\text{p err}}\rangle = \frac{1}{\sqrt{|C^{\perp}|}} \sum_{y \in C^{\perp}} (-1)^{(x+y)\cdot e_2} |x+y\rangle$$

and using the result of (f), we obtain

$$\begin{aligned} H^{\otimes n}|\psi_{\text{p err}}\rangle &= \frac{1}{\sqrt{|C^{\perp}|}} \sum_{z \in \{0,1\}^n} \sum_{y \in C^{\perp}} (-1)^{(x+y)\cdot(e_2+z)} |z\rangle \\ &= \frac{1}{\sqrt{|C^{\perp}|}} \sum_{z' \in \{0,1\}^n} \sum_{y \in C^{\perp}} (-1)^{(x+y)\cdot z'} |z'+e_2\rangle \\ &= \sum_{z' \in C^{\perp}} \sum_{y \in C^{\perp}} (-1)^{(x+y)\cdot z'} |z'+e_2\rangle . \end{aligned}$$

If we now use the check matrix for code $C^{\perp}$, i.e. G^T, we obtain the binary expression for error e_2. We flip the bit and perform $H^{\otimes n}$ again to obtain the error corrected original state $|\psi(x)\rangle$.