18.435/2.111 Homework # 3 Solutions

Solution to 1:
For $N = 15$, $\frac{3}{4}$ of the possible x's with $\gcd(x, 15) = 1$ yield an r that is even and with $x^{r/2} \neq -1$. For $N = 63$, $\frac{1}{2}$ of the residues yield such an r. One way to do this is to use the Chinese remainder theorem. I will do $N = 15$ in detail so that people can see what is happening, and then give a shorter way of figuring out the answer for $N = 63$.

For $N = 15$, we will need to look at the x's modulo 3 and modulo 5. Consider the following table.

$x \pmod 3$	r_3	x (mod 5)	r_5	r	$x^{r/2} \pmod 3$	$x^{r/2} \pmod 5$
1	1	1	1	1	—	—
-1	2	1	1	2	-1	1
1	1	2	4	4	1	-1
-1	2	2	4	4	1	-1
1	1	3	4	4	1	-1
-1	2	3	4	4	1	-1
1	1	-1	2	2	1	-1
-1	2	-1	2	2	-1	-1

We found r by taking the least common multiple of r_3 and r_5. Everything else in the table should be fairly self-evident. Note that $x^{r/2} \pmod 3$ and $x^{r/2} \pmod 5$ are either 1 or -1. This has to be the case, since their squares are 1 and the only square roots of 1 modulo an odd prime p are ± 1 [this is a consequence of the muliplicative group modulo the prime being cyclic].

The procedure fails either if both the r's are odd, or if both $x^{r/2} \pmod 3$ and $x^{r/2} \pmod 5$ are -1.

Now, let's condider the case of 63. We give the relatively prime residues (mod 9) and (mod 7) and their orders r_9 and r_7 in the tables below:

r_7	residues
1	1 (mod 7)
2	-1 (mod 7)
3	2,4 (mod 7)
2	3,5 (mod 7)

r_9	residues
1	1 (mod 9)
2	-1 (mod 9)
3	4,7 (mod 9)
2	2,5 (mod 9)

In this case, the algorithm will fail if both r_7 and r_9 are odd, or if both r_7 and r_9 are even. It is easy to see that the probability that this happens is $\frac{1}{2}$.

The algorithm fails when both r_y and r_9 are odd because then r is odd. Why does it fail when they're both even? We have $r/2 = \mathrm{lcm}(r_7, r_9)/2$ is odd, and $x^{r_7/2} \equiv -1 \pmod 7$ and $x^{r_9/2} \equiv -1 \pmod 9$. Thus, $r/2 = (r_7/2)t$ for some odd integer t, and

$$x^{r/2} \equiv (x^{r_7/2})^t \equiv (-1)^t \equiv -1 \bmod 7$$

and similarly (mod 9).

Now, suppose r_7 is even and r_9 is odd. Then $r/2 = (r_7/2)t_7$ for some odd integer t, and $r/2 = r_9 t_9$ for some odd integer t_9. The argument above can be adapted to show that $x^{r_7} \equiv -1 \pmod 7$ but $x^{r_9} \equiv 1 \pmod 9$, and the factoring algorithm works.

One could also use the statement from the proof of Theorem A4.13 in Nielsen and Chuang, which says that the algorithm will fail for a number $N = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m}$ exactly when the largest powers of two dividing all the r_i are equal. Using the fact that multiplication modulo p^α forms a cyclic group for odd primes p and a little group theory, one can show that if $p \equiv 3 \pmod 4$, for exactly half the residues mod p^α, we have r_{p^α} odd and for the other half, r_{p^α} is twice an odd number, so if $N = p_1^{\alpha_1} p_2^{\alpha_2}$ with both p_1 and p_2 congruent to 3 modulo 4, the factoring algorithm chooses a bad x with probability $\frac{1}{2}$.

Problem 2: Suppose we try to apply the factoring algorithm to a number $N = p^\alpha$ which is a power of p. Will it work? If not, what goes wrong.

Solution to 2: In the statement of the problem, I accidentally forgot to say explicitly that p was prime, which is the case I meant you to consider. If p is not prime, the algorithm works fine. If p is prime, then you run into the problem that the only square roots of 1 modulo p^α are $+1$ and -1. Thus, $x^r \equiv 1 \pmod{p^\alpha}$ forces us to have $x^{r/2} \equiv -1 \pmod{p^\alpha}$. [We can't have $x^{r/2} \equiv 1 \pmod{p^\alpha}$ since r was the minimum power giving $x^r \equiv 1$]. This doesn't give us two numbers $a^2 \equiv b^2 \pmod{p^\alpha}$ with $x \not\equiv \pm y$, so we don't get a factorization.

Problem 3: Suppose we try to apply the factoring algorithm, but we forget to check whether $\gcd(x, N) = 1$ and accidentally choose an x with $1 < x < N$ and $\gcd(x, N) > 1$. Will the algorithm still work? If not, what goes wrong?

Solution to 3: In the algorithm, we need to construct the unitary transformation U acting on $|\,a\rangle$ for $0 \leq a < N$ as $U\,|\,a\rangle = |\,ax \bmod N\rangle$. This transformation is not unitary if $\gcd(x, N) > 1$. To see this, note that there are two unequal residues a_1 and $a_2 < N$ such that $a_1 x \bmod N = a_2 x \bmod N$. To see this explicitly, consider a prime p dividing both x and N. The transformation U has to take both $|\,a_1\rangle = |\,0\rangle$ and $|\,a_2\rangle = |\,N/p\rangle$ to $|\,0\rangle$.

Solution to 4:
We have

$$\tilde{f} = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{-2\pi i \ell x/N} f(x).$$

Now, let's write $x = ry + z$ where $0 \leq z < r$. We can rewrite the sum above

$$\tilde{f} = \frac{1}{\sqrt{N}} \sum_{z=0}^{r-1} \sum_{y=0}^{N/r-1} e^{-2\pi i \ell (ry+z)/N} f(ry+z).$$

Breaking the exponential in two parts and using the fact that $f(ry+z) = f(z)$, we get

$$\tilde{f} = \frac{1}{\sqrt{N}} \sum_{z=0}^{r-1} e^{-2\pi i \ell z/N} f(z) \sum_{y=0}^{N/r-1} e^{-2\pi i \ell r y/N}$$

The second piece is just 0 unless ℓ is an integer multiple of N/r, in which case it is N/r [the book has a typo]. This gives

$$\tilde{f} = \frac{\sqrt{N}}{r} \sum_{z=0}^{r} e^{-2\pi i \ell(z)/N} f(z).$$

if ℓ is an integer multiple of N/r and 0 otherwise.

The part about relating the result to 5.63 was fairly vague, and several students had questions about it. What I assume Nielsen and Chuang wanted you to do was use it to prove the approximation in Step 3 of the period-finding algorithm. You can do this by breaking the sum on x from 0 to $2^t - 1$ into two parts, where the first part runs from 0 to $N-1$ where N is an integer multiple of r and the second part contains the remaining terms.

Solution to 5. The period-finding algorithm doesn't work well for the function

$$\begin{aligned} f(x) &= 1 \qquad \text{if } r \text{ divides } x \\ f(x) &= 0 \qquad \text{if } x \text{ is not a multiple of } r. \end{aligned}$$

Let's analyze it. We have the superposition

$$\frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |\,x\rangle\,|\,f(x)\rangle$$

and we take the inverse Fourier transform of it. This is

$$\frac{1}{2^t} \sum_{x=0}^{2^t-1} \sum_{y=0}^{2^t-1} e^{-2\pi i x y/2^t}\,|\,y\rangle\,|\,f(x)\rangle$$

This sum splits into two parts, the case where $f(x) = 0$ and the case where $f(x) = 1$. Let's do the case where $f(x) = 0$ first. We get that the amplitude on the state $|\,y\rangle\,|\,0\rangle$ is:

$$\frac{1}{2^t} \sum_{\substack{x=0 \\ r \text{ does not divide } x}}^{2^t-1} e^{-2\pi i x y/2^t}$$

Suppose $y = 0$. Then, all the terms in this sum are 1, and there are roughly $(r-1)/r$ terms in the sum, since we get one term for all the x that are not integer multiples of r. Thus, the amplitude of the sum is around $(r-1)/r$, and the probability of seeing $|\,0\rangle\,|\,0\rangle$ is the square of the amplitude, or approximately $(r-1)^2/r^2 \approx 1 - 2/r$. This outcome doesn't tell us anything about r, since it says that $0/2^t$ is a fraction close to $0/r$, which is true for any r. Now, suppose $y \neq 0$. We again have the amplitude

$$\frac{1}{2^t} \sum_{\substack{x=0 \\ r \text{ does not divide } x}}^{2^t-1} e^{-2\pi i x y/2^t}.$$

We can analyze this by breaking it into two sums as follows

$$\frac{1}{2^t}\left(\sum_{x=0}^{2^t-1} e^{-2\pi ixy/2^t} - \sum_{\substack{x=0\\ r \text{ divides } x}}^{2^t-1} e^{-2\pi ixy/2^t}\right).$$

If $y \neq 0$, the first sum is 0, so we need only to analyze the second sum. Changing the index of summation, this is

$$-\frac{1}{2^t}\sum_{x'=0}^{(2^t-1)/r} e^{-2\pi irx'y/2^t},$$

which is the same sum we saw in the phase estimation algorithm. By the same analysis, we find that if $y/2^t$ is close to a fraction d/r, the sum has a value close to $2^t/r$, and if $y/2^t$ is far from a fraction d/r, the sum has a negligible value. Thus, for each of the $r-1$ fractions d/r, $d \neq 0$, we obtain a y with $y/2^t \approx d/r$ with probability $1/r^2$. From most of these fractions we will be able to recover r, so this case usually succeeds, but this case only occurs with probability around $1/r$.

If $f(x) = 1$, then x must be a multiple of r, and the amplitude is

$$\frac{1}{2^t}\sum_{\substack{x=0\\ r \text{ divides } x}}^{2^t-1} e^{-2\pi ixy/2^t}.$$

This sum is the same as for the case where $y \neq 0$ and $f(x) = 0$, so this case again occurs with probability approximately $1/r$, and if we are in this case we succeed most of the time.

The period-finding algorithm thus succeeds for this f with probability approximately $2/r$. The large failure probability is due to this function essentially having period 1, or more precisely, its being very close to a function with period 1. The Fourier tranform picks out this period with high probability, and the period of r with only fairly low probability.

Solution to 6: Recall the geometric description of Grover's algorithm, where we have a basis in which ψ rotates by an angle of θ with each iteration. We start with an angle of $\theta/2$, and we a target set with probability 1 when $\theta = \pi/2$. Thus, we want $3\theta/2 = \pi/2$, or $\theta/2 = \pi/6$. But recall

$$\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}.$$

This gives $M/N = 1/4$.

Solution to 7: Let the target set be T. Define

$$\begin{aligned} |\,\beta\rangle &= \frac{1}{\sqrt{M}}\sum_{x\in T}|\,x\rangle \\ |\,\alpha\rangle &= \frac{1}{\sqrt{N-M}}\sum_{x\notin T}|\,x\rangle \\ |\,\psi\rangle &= \frac{1}{\sqrt{N}}\sum_{x}|\,x\rangle \end{aligned}$$

Then we have that the starting state

$$|\,\psi\rangle = \frac{\sqrt{M}}{\sqrt{N}}|\,\beta\rangle + \frac{\sqrt{N-M}}{\sqrt{N}}|\,\alpha\rangle$$

and after the first step

$$O\,|\,\psi\rangle = e^{i\phi}\frac{\sqrt{M}}{\sqrt{N}}|\,\beta\rangle + \frac{\sqrt{N-M}}{\sqrt{N}}|\,\alpha\rangle\,.$$

Now, note the inner products

$$\begin{aligned} \langle\beta|\psi\rangle &= \frac{\sqrt{M}}{\sqrt{N}} \\ \langle\alpha|\psi\rangle &= \frac{\sqrt{N-M}}{\sqrt{N}} \end{aligned}$$

Also, note that

$$H^{\otimes n}[(1-e^{i\phi})\,|\,0\rangle\langle 0\,| - I]H^{\otimes n} = (1-e^{i\phi})\,|\,\psi\rangle\langle\psi\,| - I$$

Thus, we get that

$$\tilde{G}\,|\,\psi\rangle \;=\; (1-e^{i\phi})(\frac{M}{N}e^{i\phi} + \frac{N-M}{M})(\frac{\sqrt{N-M}}{N}|\,\alpha\rangle + \frac{\sqrt{M}}{\sqrt{N}}|\,\beta\rangle) - e^{i\phi}|\,\beta\rangle - |\,\alpha\rangle$$

We can now pull off the coefficients on $|\,\alpha\rangle$ and $|\,\beta\rangle$. We find that we get

$$e^{i\phi}(-\frac{M}{N}2\cos\phi - \frac{N-2M}{N})\sqrt{\frac{N-M}{N}}\,|\,\alpha\rangle$$

which can be made 0 for the appropriate choice of ϕ, provided M is between $N/4$ and N.

A generalization of this technique shows that if you known M, and choose the appropriate number of Grover iterations followed by one of these iterations, you can put all the amplitude on the target states.

18.435/2.111 Homework # 4 Solutions

Problem 1: In the teleportation protocol, show that the probability distribution for the values of the two qubits that Alice sends to Bob is independent of the state ψ of the qubit being transmitted.

Solution to 1:

There are many ways of doing this problem. Writing everything out explicitly gives a straightforward, and not too complicated proof. This is done on page 108 of Nielsen and Chuang (something I didn't realize when I assigned the problem). Here's another proof, using properties of Pauli matrices:

Alice measures $\frac{1}{\sqrt{2}}|\,\psi\rangle \otimes (|\,01\rangle - |\,10\rangle)$ in the Bell basis. We want to show that the probability of obtaining each of the four Bell states is 1/4. The Bell basis Alice measures in consists of

$$|\,\psi_{EPR}\rangle = \frac{1}{\sqrt{2}}(|\,01\rangle - |\,10\rangle)$$

and $\sigma_b^{(2)}\,|\,\psi_{EPR}\rangle$ where $b = x, y, z$ and the superscript 2 means that the Pauli matrix is applied to the second qubit. So we want to show that the projection

$${}_{12}\langle\psi_{EPR}\,|\,{\sigma_b^{(2)}}^{\dagger}(|\,\psi\rangle_1 \otimes |\,\psi_{EPR}\rangle_{23})$$

is independent of b. (The subscripts on $\langle\,|$ and $|\,\rangle$ indicate which qubits these states describe.) This can be seen by realizing that the above measurement gives the same result as projecting the state ${\sigma_b^{(2)}}^{\dagger}(|\,\psi\rangle_1 \otimes |\,\psi_{EPR}\rangle_{23})$ onto ${}_{12}\langle\psi_{EPR}\,|$. But because applying the same change of basis to both qubits in ψ_{EPR} gives ψ_{EPR} back, we have

$${\sigma_b^{(2)}}^{\dagger}(|\,\psi\rangle_1 \otimes |\,\psi_{EPR}\rangle_{23}) = \sigma_b^{(3)}(|\,\psi\rangle_1 \otimes |\,\psi_{EPR}\rangle_{23})$$

and the probability that Alice obtains ${}_{12}\langle\psi_{EPR}\,|$ when she measures this state in the Bell basis cannot be changed if Bob applies $\sigma_b^{(3)}$ to his qubit. Thus, all the probabilities must be equal.

Solution 2:

Alice and Bob share four qubits in the state

$$\frac{1}{2}\,(|\,0000\rangle + |\,0101\rangle + |\,1010\rangle - |\,1111\rangle)$$

This state is just $S(|\,\psi_{EPR}\rangle \otimes |\,\psi_{EPR}\rangle)$, where S is a controlled σ_z. If Alice takes a two-qubit state $|\,\phi\rangle$ and performs the regular teleportation protocol on her two qubits, Bob ends up with

$$S(\sigma_b^{(1)} \otimes \sigma_b^{(2)})\,|\,\phi\rangle\,,$$

where σ_b is either the identity or one of the four Pauli matrices. He now needs to convert this to $S\phi$. It is easy to see that $\sigma_z^{(i)}$ commutes with S where $i = 1, 2$, and that

$$\begin{aligned} S\sigma_x^{(1)} &= \sigma_z^{(2)}\sigma_x^{(1)}S \\ S\sigma_x^{(2)} &= \sigma_z^{(1)}\sigma_x^{(2)}S \end{aligned}$$

From these, and the relation $\sigma_y = i\sigma_x\sigma_z$, we can (assuming no calculation mistakes on my part) derive the following table.

Bob′s correction	Bob′s correction
in regular teleportation	teleporting through S
id	id
$\sigma_x^{(2)}$	$\sigma_z^{(1)} \otimes \sigma_x^{(2)}$
$\sigma_y^{(2)}$	$\sigma_z^{(1)} \otimes \sigma_y^{(2)}$
$\sigma_z^{(2)}$	$\sigma_z^{(2)}$
$\sigma_x^{(1)}$	$\sigma_x^{(1)} \otimes \sigma_z^{(2)}$
$\sigma_x^{(1)} \otimes \sigma_x^{(2)}$	$\sigma_y^{(1)} \otimes \sigma_y^{(2)}$
$\sigma_x^{(1)} \otimes \sigma_y^{(2)}$	$\sigma_y^{(1)} \otimes \sigma_x^{(2)}$
$\sigma_x^{(1)} \otimes \sigma_z^{(2)}$	$\sigma_x^{(1)}$
$\sigma_y^{(1)}$	$\sigma_y^{(1)} \otimes \sigma_z^{(2)}$
$\sigma_y^{(1)} \otimes \sigma_x^{(2)}$	$\sigma_x^{(1)} \otimes \sigma_y^{(2)}$
$\sigma_y^{(1)} \otimes \sigma_y^{(2)}$	$\sigma_x^{(1)} \otimes \sigma_x^{(2)}$
$\sigma_y^{(1)} \otimes \sigma_z^{(2)}$	$\sigma_y^{(1)}$
$\sigma_z^{(1)}$	$\sigma_z^{(1)}$
$\sigma_z^{(1)} \otimes \sigma_x^{(2)}$	$\sigma_x^{(2)}$
$\sigma_z^{(1)} \otimes \sigma_y^{(2)}$	$\sigma_y^{(2)}$
$\sigma_z^{(1)} \otimes \sigma_z^{(2)}$	$\sigma_z^{(1)} \otimes \sigma_z^{(2)}$

The mapping between Alice's measurement and Bob's correction is now straightforward to compute, given the map between Alice's mesurement and Bob's correction in regular teleportation.

Problem 3:
If Alice and Bob share a set of qutrits in the state

$$\frac{1}{\sqrt{3}}(|\,00\rangle + |\,11\rangle + |\,22\rangle),$$

show that Alice can do superdense coding by applying R^aT^b to this state, for $0 \leq a \leq 2$ and $0 \leq b \leq 2$, where

$$T = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{and} \quad R = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}$$

where $\omega = e^{2\pi i/3}$. Note that I left out the definition of ω in the problem set, but most people figured it out.
Solution to 3: We need to show that

$$\langle EPR_3\,|\,(T^{\dagger^{b'}}R^{\dagger^{a'}} \otimes I)(R^aT^b \otimes I)\,|\,EPR_3\rangle = \delta_{a-a'}\delta_{b-b'}$$

where δ is the Kronecker δ function. This will show that the nine states Alice produces are an orthonormal basis, so when she sends her qutrit to Bob, he can distinguish all nine states using a von Neumann measurement. We can use the fact that $R^3 = T^3 = I$ and that $TR = \omega RT$ to simplify

$$T^{\dagger b'} R^{\dagger a'} R^a T^b = \omega^{-b'(a-a')} R^{a-a'} T^{b-b'} .$$

This means we merely need to show that

$$\langle EPR_3 \,|\, R^a T^b \otimes I \,|\, EPR_3 \rangle = \delta_a \delta_b$$

for $0 \leq a, b \leq 2$. If $b \neq 0$, then $R^a T^b \otimes I \,|\, EPR_3 \rangle$ is a superposition of basis states of the form $|\, ij \rangle$ for $i \neq j$, and so has inner product 0 with $|\, EPR_3 \rangle$. If $b = 0$, then

$$R^a \,|\, EPR_3 \rangle = \frac{1}{\sqrt{3}} (|\, 00 \rangle + \omega^a \,|\, 11 \rangle + \omega^{2a} \,|\, 22 \rangle)$$

and the inner product of this with $|\, EPR_3 \rangle$ is $(1 + \omega^a + \omega^{2a})/3$, which if we choose $\omega = e^{2\pi i/3}$ is 1 if $a = 0$, and 0 if $a = 1, 2$.

Solution for 4: Alice and Cathy share a Bell state, which can be written as

$$\sigma_1^{(C)} \,|\, \psi_{EPR} \rangle_{AC} ,$$

where σ_1 is either one of the three Pauli matrices or the identity. The (C) represents that it is applied to Cathy's qubit [note that this really should be written $id^{(B)} \otimes \sigma_1^{(C)}$, but we are leaving out implied identity matrices, as this notation gets cumbersome very quickly]. Alice and Cathy don't know what σ_1 is, but they know that it is the same as the σ_1 in the state Bob and David share, which is

$$\sigma_1^{(D)} \,|\, \psi_{EPR} \rangle_{BD} .$$

Now, if Alice uses

$$\sigma_1^C \,|\, \psi_{EPR} \rangle_{AC}$$

to teleport her qubit of $|\, \psi_{EPR} \rangle_{AB}$ to Cathy, what happens is that Cathy and Bob now hold $\sigma_1^C \sigma_2^C \,|\, \psi_{EPR} \rangle_{CB}$, where Cathy knows what σ_2^C is (because this depends on the results of Alice's measurement) but not σ_1. Now, Bob uses

$$\sigma_1^D \,|\, \psi_{EPR} \rangle_{BD}$$

to teleport his qubit of $\sigma_1^C \sigma_2^C \,|\, \psi_{EPR} \rangle_{CB}$ to David. Now, Cathy and David share

$$\sigma_1^C \sigma_2^C \otimes \sigma_1^D \sigma_3^D \,|\, \psi_{EPR} \rangle_{CD} = \pm \sigma_2^C \sigma_1^C \otimes \sigma_3^D \sigma_1^D \,|\, \psi_{EPR} \rangle_{CD} ,$$

where we can interchange the two pairs of Pauli matrices because any two Pauli matrices either commute or anticommute. But since Cathy and David know σ_2 and σ_3, they can undo them, leaving

$$\pm \sigma_1^C \otimes \sigma_1^D \,|\, \psi_{EPR} \rangle_{CD} .$$

The ± 1 phase factor does not change the quantum state, and since the state $|\,\psi_{EPR}\rangle_{CD}$ is invariant when the same basis transformation is applied to both of its qubits, Cathy and David now share

$$\pm\,|\,\psi_{EPR}\rangle_{CD}\,,$$

which is what we wanted.

Problem 5. It's late, and problem 5 is not only extra credit, but also quite tricky, so I'll post the solution to it later.

18.435/2.111 Homework # 5 Solutions

Solution to 1: We want

$$\frac{1}{3}\left(|\,0\rangle\langle 0\,| + \frac{1}{4}(|\,0\rangle + \sqrt{3}\,|\,1\rangle)(\langle 0\,| + \sqrt{3}\,\langle 1\,|) + \frac{1}{4}(|\,0\rangle - \sqrt{3}\,|\,1\rangle)(\langle 0\,| - \sqrt{3}\,\langle 1\,|)\right)$$

which is

$$\frac{1}{3}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{12}\begin{pmatrix} 1 & \sqrt{3} \\ \sqrt{3} & 3 \end{pmatrix} + \frac{1}{12}\begin{pmatrix} 1 & -\sqrt{3} \\ -\sqrt{3} & 3 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Solution to 2: When we take the partial trace over the second qubit of the state

$$\frac{1}{\sqrt{3}}\left(|\,00\rangle + |\,01\rangle + |\,10\rangle\right),$$

we can compute the density matrix of the above state

$$\frac{1}{3}\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

and taking the partial trace explicitly, we obtain

$$\frac{1}{3}\begin{pmatrix} \mathrm{Tr}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} & \mathrm{Tr}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \\ \mathrm{Tr}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} & \mathrm{Tr}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \end{pmatrix} = \frac{1}{3}\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

Solution to 3:
After we apply the controlled σ_z to

$$|\,\psi\rangle \otimes \left(\frac{\sqrt{3}}{2}\,|\,0\rangle + \frac{1}{2}\,|\,1\rangle\right)$$

we get the state

$$\frac{\sqrt{3}}{2}\,|\,\psi\rangle \otimes |\,0\rangle + \frac{1}{2}\sigma_z\,|\,\psi\rangle \otimes |\,1\rangle\,.$$

Now, we can take the partial trace by measuring the second qubit in the $|\,0\rangle\,, |\,1\rangle$ basis and using the resulting states of the first qubit and their probabilities to compute the density matrix of the second qubit. If we do this with the above state, we get

$$\frac{3}{4}\,|\,\psi\rangle\langle\psi\,| + \frac{1}{4}\sigma_z\,|\,\psi\rangle\langle\psi\,|\,\sigma_z^\dagger$$

which is easy to see how to write in operator sum notation. We get

$$A_1 = \frac{\sqrt{3}}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad A_2 = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Using a different measurement on the second qubit gives alternative operator sum decompositions.

Solution to 4:
We want to compose two noisy operations. The first one takes

$$\rho \to \sum_i B_i \rho B_i^\dagger$$

where

$$B_1 = \sqrt{1-p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad B_2 = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

and the second one takes

$$\rho \to \sum_i A_i \rho A_i^\dagger$$

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-q} \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 0 & \sqrt{q} \\ 0 & 0 \end{pmatrix}.$$

Putting them together, one sees the four operations in the operator sum notation are A_1B_1, A_1B_2, A_2B_1, and A_2B_2. However,

$$A_2B_1 = \sqrt{1-p}A_2 \quad \text{and} \quad A_2B_2 = -\sqrt{p}A_2$$

These can be combined into one operation, since

$$\begin{aligned} A_2B_1\rho B_1^\dagger A_2^\dagger + A_2B_2\rho B_2^\dagger A_2^\dagger &= (1-p)A_2\rho A_2^\dagger + pA_2\rho A_2^\dagger \\ &= A_2\rho A_2^\dagger. \end{aligned}$$

Thus, we get a noisy quantum operation with an operator-sum expression having just three operators:

$$A_1B_1 = \sqrt{1-p}\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-q} \end{pmatrix} \qquad A_1B_2 = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & -\sqrt{1-q} \end{pmatrix}. \qquad A_2 = \begin{pmatrix} 0 & \sqrt{q} \\ 0 & 0 \end{pmatrix}.$$

Solution to 5:
We can rewrite the depolarizing operation $\mathcal{D}$ as

$$\mathcal{D}(\rho) = (1 - \frac{4p}{3})\rho + \frac{4p}{3}\frac{I}{2}$$

Using this formulation, it is clear that if the eigenvalues of ρ are a and b, the eigenvalues of $\mathcal{D}(\rho)$ are $(1-4p/3)a + 2p/3$ and $(1-4p/3)b + 2p/3$. (If it's not clear, consider that when you change the basis to diagonalize ρ, the above formulation is unchanged.) Since $a, b \geq 0$, the eigenvalues of $\mathcal{D}(\rho)$ are larger than $2p/3$.

Solution to 6:
Reformulating the problem, we want to find the relation between

$$|\, x + C_2\rangle = \sum_{y \in C_2} |\, x + y\rangle$$

and

$$|\, x + C_2\rangle_{u,v} = \sum_{y \in C_2} (-1)^{u \cdot y} \,|\, x + y + v\rangle \,.$$

Suppose we take the first code $|\, x + C_2\rangle$ and first apply a σ_z to all the qubits that are 1's in u, and then a σ_x to the position of all the 1's in v. we get

$$|\, x + C_2\rangle_\alpha = \sum_{y \in C_2} (-1)^{u \cdot (x+y)} \,|\, x + y + v\rangle \,.$$

This is

$$(-1)^{u \cdot x} \,|\, x + C_2\rangle_{u,v} \,.$$

Thus, the second CSS code (with u, v) can be obtained by first applying a unitary transformation U_u to the state being encoded, then encoding it using the first CSS code, and finally applying σ_z to some encoding qubits and σ_x to other encoding qubits. This unitary transformation U_u is

$$|\, x + C_2\rangle \rightarrow (-1)^{u \cdot x} \,|\, x + C_2\rangle \,.$$

Applying a unitary transformation to the encoded state doesn't affect the error correcting properties of the code, since the code is supposed to protect all allowed codewords. Applying the Pauli matrices σ_x and σ_z to specific qubits in the code also doesn't affect the overall error correcting properties of the code, since up to a possible overall -1 sign in the global phase, this operation takes phase errors to phase errors and bit errors to bit errors.