Solutions for Problem Sheet 4

C7.4 Introduction to Quantum Information – HT 2020 – A. Ekert & J. Mur-Petit

1 CP maps revisited

1) For the transposition map we have,

$$\tilde{T} = \left[\begin{array}{c|c} |0\rangle\langle 0| & |1\rangle\langle 0| \\ \hline |0\rangle\langle 1| & |1\rangle\langle 1| \end{array}\right]$$

2) For the depolarising channel $\varrho \mapsto (1-p)\varrho + \frac{p}{3}\left(\sigma_x\varrho\sigma_x + \sigma_y\varrho\sigma_y + \sigma_z\varrho\sigma_z\right)$ either use 3.5 part (2) from the previous sheet, or recall that

$$\begin{aligned} \sigma_z|0\rangle &= |0\rangle\,, & \sigma_x|0\rangle &= |1\rangle\,, & \sigma_y|0\rangle &= i|1\rangle\,, \\ \sigma_z|1\rangle &= -|1\rangle\,, & \sigma_x|1\rangle &= |0\rangle\,, & \sigma_y|1\rangle &= -i|0\rangle \end{aligned}$$

to evaluate the map directly and find

$$\tilde{T} = \left[\begin{array}{c|c} \left(1-\frac{2p}{3}\right)|0\rangle\langle 0| + \frac{2p}{3}|1\rangle\langle 1| & \left(1-\frac{4p}{3}\right)|0\rangle\langle 1| \\ \hline \left(1-\frac{4p}{3}\right)|1\rangle\langle 0| & \frac{2p}{3}|0\rangle\langle 0| + \left(1-\frac{2p}{3}\right)|1\rangle\langle 1| \end{array}\right]$$

To show the positive semi-definiteness of $\tilde{T}$ we have to check that for any complex vector c we have

$$c^\dagger \tilde{T} c \geq 0$$

First note that for each submatrix we can write the output in the standard basis as,

$$T(|a\rangle\langle b|) = \sum_{\alpha,\beta=0,1} T_{(a\alpha)(b\beta)}|\alpha\rangle\langle\beta|$$

The coefficients are therefore given by,

$$T_{(a\alpha)(b\beta)} = \langle\alpha|T(|a\rangle\langle b|)|\beta\rangle$$

Now, for CP maps

$$T(|a\rangle\langle b|) = \sum_k A_k|a\rangle\langle b|A_k^\dagger\,, \quad \sum_k A_k A_k^\dagger = \sum_k A_k^\dagger A_k = \mathbb{1}$$

hence

$$T_{(a\alpha)(b\beta)} = \sum_k \langle\alpha|A_k|a\rangle\langle b|A_k^\dagger|\beta\rangle \tag{1}$$

We could write $\tilde{T}$ as a sum of matrices made up of terms for a fixed k, i.e. $\tilde{T} = \sum_k \tilde{T}^k$ where the components for a fixed k are given by $T^k_{(a\alpha)(b\beta)} = \langle\alpha|A_k|a\rangle\langle b|A_k^\dagger|\beta\rangle$. From Eq. (1), we have that each such term $T^k_{(a\alpha)(b\beta)}$ is of the form $v_i v_j^*$ for $(i = a\alpha, j = b\beta)$. Thus we can write the condition for positive semi-definiteness for the $\tilde{T}^k$ matrices as

$$c^\dagger\tilde{T}^k c = \sum_{i,j} c_i^* v_i v_j^* c_j = \langle c|v\rangle\langle v|c\rangle = |\langle c|v\rangle|^2 \geq 0$$

where we recognised that for any complex vectors $|c\rangle = [c_1, c_2, .., c_n]^T$, $|v\rangle = [v_1, v_2, .., v_n]^T$ then

$$\langle c|v\rangle = \sum_i c_i^* v_i$$

This means the total matrix is the sum over k of these positive semidefinite matrices which means it itself is positive semidefinite.

Bonus material: Let's quickly say something more about this $\tilde{T}$ matrix. Whilst it is clear that this mathematical object encodes all of the information about the transformation T it is not immediately clear what, if any, other interpretation this matrix might have. In fact, it possesses a very nice operational interpretation and is part of an incredibly useful trick called the *Choi isomorphism*[1] that has many applications in quantum information theory.

Imagine Alice has the state

$$|\tilde{\Phi}\rangle_{AB} = \sum_{j=0}^{d-1} |j\rangle_A |j\rangle_B$$

where $\{|j\rangle\}$ are computational basis states in d-dimensions and we have written the tilde to emphasise that this is an unnormalised and hence unphysical state (don't worry about this for now). For two dimensions this would be an unnormalised Bell state $|\tilde{\Phi}\rangle_{AB} = |00\rangle + |11\rangle$. Now imagine she sends one system to Bob during which it is transformed by T. This can be written

$$\begin{aligned}
(\mathbb{1}_A \otimes T_B)(|00\rangle + |11\rangle)(\langle 00| + \langle 11|) &= (\mathbb{1}_A \otimes T_B)(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|) \\
&= |0\rangle\langle 0| \otimes T(|0\rangle\langle 0|) + |0\rangle\langle 1| \otimes T(|0\rangle\langle 1|) \\
&+ |1\rangle\langle 0| \otimes T(|1\rangle\langle 0|) + |1\rangle\langle 1| \otimes T(|1\rangle\langle 1|)
\end{aligned}$$

It is straightforward to check that the above expression is precisely the matrix $\tilde{T}$ as defined in the question.

In a nutshell, this is the heart of the Choi result, namely that there is an isomorphism between a channel from Alice to Bob (i.e. the map $T : \mathcal{H}_A \to \mathcal{H}_B$) and a joint 'state' shared between Alice and Bob (the state $\tilde{T} \in \mathcal{H}_A \otimes \mathcal{H}_B$). This state is obtained by applying the map to one part of a maximally entangled state. If the map is a CP map, we should expect it to map physical states to physical states. If we had started with a normalised, physical state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ in the above calculation we would have ended up with a factor $\frac{1}{2}$ out the front (or $\frac{1}{d}$ more generally). You can check that, for CP maps, this would have resulted in a $\tilde{T}$ matrix with trace equal to one. And you have just proven that if the map is CP then the $\tilde{T}$ matrix is positive semidefinite thus confirming our expectations. One caveat about the Choi isomorphism is that it is defined in a basis-dependent way (e.g., above we used the computational basis). The Jamiolkowski isomorphism avoids this, but at the cost of not always mapping to a physical joint state for CP maps. Some further discussion about this issue and other interpretations of the Choi-Jamiolkowski isomorphism can be found in *Classical to Quantum Shannon Theory* by Mark Wilde[2] or this very readable blog post by Matt Leifer[3].

2 Quantum Error correction

1) A controlled-NOT gate with the target prepared in $|0\rangle$ implements this encoding.

$$(\alpha|0\rangle + \beta|1\rangle)|0\rangle \overset{\text{C-NOT}}{\mapsto} \alpha|00\rangle + \beta|11\rangle$$

2) Given the bit-flip errors, there are four possible scenarios: no errors, error on the first qubit, error on the second qubit, and two errors. The action of the network in each of these four cases is:

$$\begin{aligned}
(\alpha|00\rangle + \beta|11\rangle)|0\rangle &\mapsto (\alpha|00\rangle + \beta|11\rangle)|0\rangle && \text{no errors} \\
(\alpha|10\rangle + \beta|01\rangle)|0\rangle &\mapsto (\alpha|10\rangle + \beta|01\rangle)|1\rangle && \text{error on 1st qubit} \\
(\alpha|01\rangle + \beta|10\rangle)|0\rangle &\mapsto (\alpha|01\rangle + \beta|10\rangle)|1\rangle && \text{error on 2nd qubit} \\
(\alpha|11\rangle + \beta|00\rangle)|0\rangle &\mapsto (\alpha|11\rangle + \beta|00\rangle)|0\rangle && \text{error on both}
\end{aligned}$$

[1] You will more commonly read about the *Choi-Jamiolkowski* isomorphism which encompasses two similar, but distinct, results by the respective authors.

[2] Chapter 4, page 151, in https://arxiv.org/abs/1106.1445

[3] http://mattleifer.info/2011/08/01/the-choi-jamiolkowski-isomorphism-youre-doing-it-wrong/

This shows that outcome $x = 0$ is inconclusive for it occurs both in the absence of errors and when there are two errors (one on each qubit). The outcome $x = 1$ indicates one error, be it on the first or on the second qubit, which makes it impossible to correct it. The two-qubit code is an error detection but not an error correction code.

3) The Hadamard gate can be written as $H = \frac{1}{\sqrt{2}}(\sigma_z + \sigma_x)$. Thus, acting on the code state $\alpha|000\rangle + \beta|111\rangle$ it will create a superposition of two terms corresponding to the code state with a phase-flip error created by σ_z and a bit-flip error created by σ_x. For example, consider applying the Hadamard to the third qubit, which we will write H_3 using a subscript to denote the target qubit (subscript 1 corresponding to the top qubit). This results in

$$\begin{aligned}\alpha|000\rangle + \beta|111\rangle &\overset{H_3}{\mapsto} \frac{1}{\sqrt{2}}\left[\alpha|00\rangle(|0\rangle + |1\rangle) + \beta|11\rangle(|0\rangle - |1\rangle)\right] \\ &= \frac{1}{\sqrt{2}}\left[\underbrace{(\alpha|000\rangle - \beta|111\rangle)}_{\text{phase-flip error}} + \underbrace{(\alpha|001\rangle + \beta|110\rangle)}_{\text{bit-flip error on qubit 3}}\right]\end{aligned}$$

The first term corresponds to the phase-flip error which can be attributed to any of the three qubits (even though it originates from the qubit to which the Hadamard gate was applied). The second term corresponds to the bit-flip error on the qubit to which the Hadamard gate was applied (here the third qubit).
If we had applied the Hadamard to first or second qubit instead we would have found

$$\begin{aligned}\alpha|000\rangle + \beta|111\rangle &\overset{H_1}{\mapsto} \frac{1}{\sqrt{2}}\left[\underbrace{(\alpha|000\rangle - \beta|111\rangle)}_{\text{phase-flip error}} + \underbrace{(\alpha|100\rangle + \beta|011\rangle)}_{\text{bit-flip error on qubit 1}}\right] \\ \alpha|000\rangle + \beta|111\rangle &\overset{H_2}{\mapsto} \frac{1}{\sqrt{2}}\left[\underbrace{(\alpha|000\rangle - \beta|111\rangle)}_{\text{phase-flip error}} + \underbrace{(\alpha|010\rangle + \beta|101\rangle)}_{\text{bit-flip error on qubit 2}}\right]\end{aligned}$$

4) Stepping through the circuit in Fig. 2 for an error on the 3rd qubit as above gives

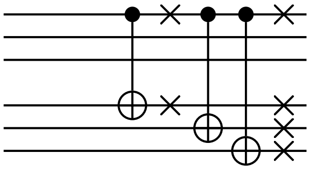
$$\begin{aligned}&\tfrac{1}{\sqrt{2}} && [(\alpha|000\rangle - \beta|111\rangle) + (\alpha|001\rangle + \beta|110\rangle)]|0\rangle|0\rangle \\ &\overset{\text{C-NOT14}}{\mapsto} && \frac{1}{\sqrt{2}}[\alpha|000\rangle|0\rangle|0\rangle - \beta|111\rangle|1\rangle|0\rangle + \alpha|001\rangle|0\rangle|0\rangle + \beta|110\rangle|1\rangle|0\rangle] \\ &\overset{\text{C-NOT24}}{\mapsto} && \frac{1}{\sqrt{2}}[\alpha|000\rangle|0\rangle|0\rangle - \beta|111\rangle|0\rangle|0\rangle + \alpha|001\rangle|0\rangle|0\rangle + \beta|110\rangle|0\rangle|0\rangle] \\ &\overset{\text{C-NOT25}}{\mapsto} && \frac{1}{\sqrt{2}}[\alpha|000\rangle|0\rangle|0\rangle - \beta|111\rangle|0\rangle|1\rangle + \alpha|001\rangle|0\rangle|0\rangle + \beta|110\rangle|0\rangle|1\rangle] \\ &\overset{\text{C-NOT35}}{\mapsto} && \frac{1}{\sqrt{2}}[\alpha|000\rangle|0\rangle|0\rangle - \beta|111\rangle|0\rangle|0\rangle + \alpha|001\rangle|0\rangle|1\rangle + \beta|110\rangle|0\rangle|1\rangle] \\ &= && \frac{1}{\sqrt{2}}[(\alpha|000\rangle - \beta|111\rangle)|0\rangle|0\rangle + (\alpha|001\rangle + \beta|110\rangle)|0\rangle|1\rangle]\end{aligned}$$

If the outcome is $x_1 = 0, x_2 = 1$ then this projects onto a state whose recovery operation is to apply a bit-flip to the third qubit. If the outcome is $x_1 = 0, x_2 = 0$ then this projects onto a state whose recovery operation is to apply a phase-flip to the any qubit. Considering errors on the other qubits a similar propagation through the circuit yields

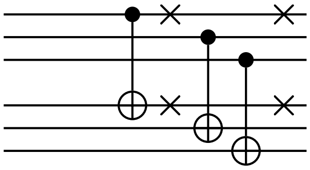
$$\begin{aligned}\frac{1}{\sqrt{2}}[(\alpha|000\rangle - \beta|111\rangle) + (\alpha|100\rangle + \beta|011\rangle)] &\mapsto \frac{1}{\sqrt{2}}[(\alpha|000\rangle - \beta|111\rangle)|0\rangle|0\rangle + (\alpha|100\rangle + \beta|011\rangle)|1\rangle|0\rangle] \\ \frac{1}{\sqrt{2}}[(\alpha|000\rangle - \beta|111\rangle) + (\alpha|010\rangle + \beta|101\rangle)] &\mapsto \frac{1}{\sqrt{2}}[(\alpha|000\rangle - \beta|111\rangle)|0\rangle|0\rangle + (\alpha|010\rangle + \beta|101\rangle)|1\rangle|1\rangle]\end{aligned}$$

Thus, we see that the result $x_1 = 0, x_2 = 0$ always corresponds to a phase-flip recovery whilst $x_1 = 1, x_2 = 0$ requires a bit flip on the first qubit and $x_1 = 1, x_2 = 1$ requires a bit-flip on the second qubit.

5) Recall that fault-tolerance of a procedure is defined as the property that if only one component in the procedure fails, then that failure causes at most one error in each encoded block of qubits output from the procedure. Errors are unrecoverable if there is more than one error in each encoded block of three qubits.
In implementation A errors can propagate through the controlled-NOT gates to violate this condition. For example, imagine an error in the first controlled-NOT gate, which will happen with probability p. This error is then propagated through both subsequent gates to contaminate the second and third qubits of the second encoded block. Thus an unrecoverable error happens with probability p.



Implementation A



Implementation B

In contrast, implementation B does not allow for error propagation and the probability of having two errors in an encoded block is of the order of p^2 since two gates would have to fail simultaneously.

3 Stabilisers define vectors and subspaces

1) We wish to show that the set $\mathcal{S}$ of stabilisers S (***unitaries*** such that $S|\psi\rangle = |\psi\rangle$) forms a group. The binary operation is the multiplication of these operators, which is associative. The identity matrix is clearly a stabiliser, and so belongs in the set. This will be the identity of the group. By unitarity, $S^\dagger S|\psi\rangle = \mathbb{1}|\psi\rangle$. Then, note that $S|\psi\rangle = |\psi\rangle$ implies that $S^\dagger|\psi\rangle = S^\dagger S|\psi\rangle = |\psi\rangle$, and thus $S^\dagger$ is also a stabiliser, and is the inverse of the group element S. Finally, we need to show closure, i.e. the multiplication of two stabilisers S and S' is again a stabiliser. This is shown by noting that $S'|\psi\rangle = |\psi\rangle$ and $S'(|\psi\rangle) = S'(S|\psi\rangle)$, thus $S'S$ is a stabiliser.

2) Take two elements of the Pauli group $P = e^{ip}\sigma_1 \otimes \sigma_2 \otimes ... \otimes \sigma_n$ and $Q = e^{iq}\tau_1 \otimes \tau_2 \otimes ... \otimes \tau_n$ where σ_j, τ_k are Pauli operators $\in \{\mathbb{1}, X, Y, Z\}$, and e^{ip}, e^{iq} are global phases. If we consider the products of two elements PQ and QP, note that

$$\begin{aligned} PQ &= e^{i(p+q)} \bigotimes_{j=1}^{n} \sigma_j \tau_j \\ QP &= e^{i(p+q)} \bigotimes_{j=1}^{n} \tau_j \sigma_j. \end{aligned}$$

Single-qubit Pauli operators either commute or anticommute, i.e. $\sigma_j\tau_j = (-1)^{x_j}\tau_j\sigma_j$ where $x_j \in \{0, 1\}$ and has the value 0 if the operators commute, and 1 if they anticommute. Therefore,

$$QP = (-1)^{\sum_{j=1}^{n} x_j} PQ,$$

so depending on $\sum_{j=1}^{n} x_j$, the n-qubit operators commute or anticommute.

3) The trace of a tensor product of two or more operators is the multiple of the trace of the individual operators, so since the stabilisers are a subgroup of the Pauli group, if there is one non-identity Pauli term for one of the tensor factors, the trace of the whole operator is 0.

The product of the two stabilisers is another stabiliser, so S^2 is a stabiliser. Since single-qubit Pauli operators square to the identity, $S^2 = e^{i(p+p)} \bigotimes_{j=1}^{n} \mathbb{1}$ where $e^{i(p+p)} \in \{i^2 = -1, 1\}$. Now, since we exclude the n-qubit Pauli operator $-\mathbb{1}$, then for the group to be closed $S^2 = \mathbb{1} \otimes \mathbb{1} \otimes ... \otimes \mathbb{1}$, and $e^{ip} \in \{\pm 1\}$.

4) Each non-identity stabiliser is a unitary operator, and since they square to the identity, they are self-adjoint and have eigenvalues $\in \{\pm 1\}$. The non-identity stabilisers have trace equal to zero, so the number of eigenvalues being equal to $+1$ is equal to the number of -1 eigenvalues. So the subspace of $+1$ eigenvectors is 2^{n-1} dimensional, and the subspace of -1 eigenvectors is 2^{n-1} dimensional, and thus splits the original space in half. The operator $\frac{1}{2}(\mathbb{1} + S)$ projects onto the $+1$ eigenspace since $\frac{1}{2}(\mathbb{1} + S)\left|\psi_{+1}\right\rangle = \frac{1}{2}\left|\psi_{+1}\right\rangle$ and $\frac{1}{2}\mathbb{1} + S)\left|\psi_{-1}\right\rangle = \frac{1}{2}(\left|\psi_{-1}\right\rangle - \left|\psi_{-1}\right\rangle) = 0$ where $\left|\psi_{\pm 1}\right\rangle$ is a ± 1 eigenstate of S, and likewise $\frac{1}{2}(\mathbb{1} - S)$ projects onto the -1 eigenspace.

5) We want to consider the intersection of the eigenspace of S_2 with the $+1$ eigenspace of S_1. So we want to consider the eigenvalues of S_2 in the $+1$ eigenspace of S_1, so $\mathrm{Tr}\frac{1}{2}(\mathbb{1} + S_1)S_2$ is the sum of the eigenvalues of S_2 in the $+1$ eigenspace of S_1.

Now we find that $\mathrm{Tr}\left[\frac{1}{2}(\mathbb{1} + S_1)S_2\right] = \frac{1}{2}(\mathrm{Tr}S_2 + \mathrm{Tr}S_3) = 0$, where $S_3 = S_1S_2$, and the result follows from $S_1 \neq S_2$, which implies that S_3 is not the identity but another stabiliser, and has trace zero. The stabiliser S_2 only has eigenvalues $\{\pm 1\}$, and we've found that its trace in the $+1$ eigenspace of S_1 must sum to 0, hence half are $+1$, and the other half are -1.

6) Every time we have an extra stabiliser S_j, the joint $+1$ eigenspace is halved. That is, the dimension of the $+1$ eigenspace is 2^{n-r}.

7) For a given state, this is a one-dimensional space, so $2^{n-r} \overset{!}{=} 1 \equiv 2^{2-2}$, and $r = 2$, i.e. we need 2 generators. The stabiliser generators for $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ respectively are $\{\mathbb{1} \otimes Z, Z \otimes \mathbb{1}\}$, $\{-\mathbb{1} \otimes Z, Z \otimes \mathbb{1}\}$, $\{\mathbb{1} \otimes Z, -Z \otimes \mathbb{1}\}$ and $\{-\mathbb{1} \otimes Z, -Z \otimes \mathbb{1}\}$. The stabiliser generators for $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$ and $|\Psi^-\rangle$ respectively are

$$\begin{aligned}&\{X \otimes X, Z \otimes Z\},\\ &\{-X \otimes X, Z \otimes Z\},\\ &\{X \otimes X, -Z \otimes Z\},\\ &\{-X \otimes X, -Z \otimes Z\}.\end{aligned}$$

8) The idea is that if we have an error then instead of getting the $+1$ eigenvalue, we get -1, and we can use this information to identify where the error happened. This is done by having anticommutation of the generators with the errors, i.e. altering the order of the operators introduces a minus sign. The errors are X errors on one of the three qubits. We also have the identity, so ideally we should tell if there were no errors. For three qubits with k generators, the dimension of the space given the generators is 2^{3-k}, so for $k = 2$ generators S_1 and S_2, we have a two-dimensional space of $+1$ eigenvectors. If we measure these (commuting) generators, then there are four measurement outcomes, two outcomes for S_1, and two outcomes for S_2. If we have the generator $S_1 = \mathbb{1} \otimes Z \otimes Z$, then it anticommutes with $E_3 = \mathbb{1} \otimes X \otimes \mathbb{1}$ and $E_4 = \mathbb{1} \otimes \mathbb{1} \otimes X$, so $S_1E_3\left|\psi_+\right\rangle = -E_3S_1\left|\psi_+\right\rangle = -E_3\left|\psi_+\right\rangle$, and likewise for E_4, with $\left|\psi_+\right\rangle$ being a $+1$ eigenstate of S_1. That is, if we have an error on the system of E_3 or E_4, the expectation of S_1 is $\left\langle\psi_+\right| E_3S_1E_3\left|\psi_+\right\rangle = -1$, and the error is detected $\mathbb{1}$.

We need to find the second generator S_2 that will give us more information. It will be $S_2 = Z \otimes Z \otimes \mathbb{1}$, since this anticommutes with E_2 and E_3. The syndrome works as follows: if we get $+1$ and $+1$ when observing both S_1 and S_2, there was no error, i.e. E_1 happened; if we get $+1$ and -1 for S_1 and S_2 respectively, then the error was E_2 and we apply an X on the first qubit; if we get -1 and $+1$ for S_1 and S_2 respectively, then the error was E_4 and we apply an X on the third qubit; finally, if we get -1 and -1 for S_1 and S_2 respectively, then the error was E_3 and we apply an X on the second qubit.

We need to find the two-dimensional codespace, i.e. the $+1$ eigenstates of S_1 and S_2. The two states

$$\frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle) \tag{2}$$

are such eigenstates, and they are orthogonal, thus defining our two-dimensional codespace. We could have constructed another code where $S_2' = Z \otimes \mathbb{1} \otimes Z$, for example, and this would have given us the same codespace, since $S_1S_2 = S_2'$.

9) The subspace will be the subspace spanned by $\{\frac{1}{\sqrt{2}}(|+++\rangle \pm |---\rangle)\}$. Expanding out we see that the

states are equal to

$$\begin{aligned}\frac{1}{\sqrt{2}}(\left|+++\right\rangle+\left|---\right\rangle) &= \frac{1}{2}(\left|000\right\rangle+\left|011\right\rangle+\left|101\right\rangle+\left|110\right\rangle)\\ \frac{1}{\sqrt{2}}(\left|+++\right\rangle-\left|---\right\rangle) &= \frac{1}{2}(\left|001\right\rangle+\left|010\right\rangle+\left|100\right\rangle+\left|111\right\rangle),\end{aligned}$$

which are the equal superposition of the parity 0 and parity 1 codeword states respectively. In this way, the two-dimensional system is encoded in the parity.

10) A state is modified by a unitary U to become $U\left|\psi\right\rangle$. Now, note that $SU^\dagger U\left|\psi\right\rangle = \left|\psi\right\rangle$, so to get the new stabiliser we conjugate it by U to get $(USU^\dagger)U\left|\psi\right\rangle = US\left|\psi\right\rangle = U\left|\psi\right\rangle$, i.e. the stabiliser becomes $USU^\dagger$.

11) The state after the first Hadamard is $\left|+\right\rangle\left|0\right\rangle$, then after the CNOT, the state is $\frac{1}{\sqrt{2}}(\left|00\right\rangle+\left|11\right\rangle)$. Finally after the phase gate, the state is $\frac{1}{\sqrt{2}}(\left|00\right\rangle+i\left|11\right\rangle)$.

In stabiliser form, the stabiliser generators of $\left|00\right\rangle$ are $\{\mathbb{1}\otimes Z, Z\otimes\mathbb{1}\}$. The Hadamard conjugates the generators to give $\{\mathbb{1}\otimes Z, HZH\otimes\mathbb{1}\} = \{\mathbb{1}\otimes Z, X\otimes\mathbb{1}\}$, and we conjugate the generators by the CNOT to get:

$$\begin{aligned}(\left|0\right\rangle\left\langle 0\right|\otimes\mathbb{1}+\left|1\right\rangle\left\langle 1\right|\otimes X)\mathbb{1}\otimes Z(\left|0\right\rangle\left\langle 0\right|\otimes\mathbb{1}+\left|1\right\rangle\left\langle 1\right|\otimes X) &= \left|0\right\rangle\left\langle 0\right|\otimes Z-\left|1\right\rangle\left\langle 1\right|\otimes Z\\ &= Z\otimes Z\\ (\left|0\right\rangle\left\langle 0\right|\otimes\mathbb{1}+\left|1\right\rangle\left\langle 1\right|\otimes X)X\otimes\mathbb{1}(\left|0\right\rangle\left\langle 0\right|\otimes\mathbb{1}+\left|1\right\rangle\left\langle 1\right|\otimes X) &= \left|0\right\rangle\left\langle 1\right|\otimes X+\left|1\right\rangle\left\langle 0\right|\otimes X\\ &= X\otimes X,\end{aligned}$$

which are indeed the stabiliser generators of $\frac{1}{\sqrt{2}}(\left|00\right\rangle+\left|11\right\rangle)$.

Finally, to apply the phase gate to X and Z respectively we get

$$\begin{aligned}(\left|0\right\rangle\left\langle 0\right|+i\left|1\right\rangle\left\langle 1\right|)(\left|0\right\rangle\left\langle 1\right|+\left|1\right\rangle\left\langle 0\right|)(\left|0\right\rangle\left\langle 0\right|-i\left|1\right\rangle\left\langle 1\right|) &= i(-\left|0\right\rangle\left\langle 1\right|+\left|1\right\rangle\left\langle 0\right|)=Y\\ (\left|0\right\rangle\left\langle 0\right|+i\left|1\right\rangle\left\langle 1\right|)(\left|0\right\rangle\left\langle 0\right|-\left|1\right\rangle\left\langle 1\right|)(\left|0\right\rangle\left\langle 0\right|-i\left|1\right\rangle\left\langle 1\right|) &= \left|0\right\rangle\left\langle 0\right|-\left|1\right\rangle\left\langle 1\right|=Z,\end{aligned}$$

thus the generators will be $\{X\otimes Y, Z\otimes Z\}$.

4 Shor's 9-qubit code

The stabilisers of Shor's 9-qubit code are:

$$\begin{aligned}S_1 &= Z_1Z_2\\ S_2 &= Z_1Z_3\\ S_3 &= Z_4Z_5\\ S_4 &= Z_4Z_6\\ S_5 &= Z_7Z_8\\ S_6 &= Z_7Z_9\\ S_7 &= X_1X_2X_3X_4X_5X_6\\ S_8 &= X_1X_2X_3X_7X_8X_9.\end{aligned}$$

Note that any single-qubit error can be decomposed into a phase flip and a bit flip, since X, Z and $XZ=-iY$ (along with the identity) form a basis of operators acting on a qubit. So for this code to correct any single-qubit error, we want that for each qubit j, there is a stabiliser generator that anticommutes with Z_j and another that anticommutes with X_j.

Now note that the first six stabilisers will identify **bit-flip errors** on any one of the qubits. For example, if the first qubit is flipped, then both S_1 and S_2 give the outcome -1. Depending on the outcomes, we apply a bit-flip to the relevant qubit to get back to the original state.

The codespace of this code is:

$$\begin{aligned}|0_c\rangle &= \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)\\ |1_c\rangle &= \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle).\end{aligned}$$

Note that the states are products of three blocks of three qubits. If there is a **sign flip** of a qubit, this will just result in a sign flip in one of the blocks, and the generators S_7 and S_8 anticommute with this sign flip. For example, if S_7 and S_8 both give outcomes -1, then there was a sign flip in the first block, but if only one of these generators gives -1, then there was a sign flip in the second block if S_7 gives -1, and a sign flip in the third block if S_8 gives -1. Depending on the outcomes, we only need to apply a Pauli-Z operator to the first qubit in the relevant block to get back to the original state.

Therefore, by measuring all 8 generators, we can correct for arbitrary single-qubit errors.

Let's go through each of the candidate two-qubit errors:

- X_1X_3 only anticommutes with S_1 so it cannot be distinguished from a bit-flip error on the second qubit, and if we apply X to the second qubit, then $|0_c\rangle$ is returned to normal but $|1_c\rangle \to -|1_c\rangle$, so we do not get back to the original state
- X_2X_7 anticommutes with S_1 and both S_5 and S_6, but nothing else. Therefore, it is possible to correct this error, since we can identify the individual bit-flips
- X_5Z_6 anticommutes with S_3 and S_7. So we can identify a bit-flip on qubit 5, and a phase-flip in the second block, and then correct for them by flipping qubit 5 and applying a phase flip to, say, the first qubit in the second block
- Z_5Z_6 commutes with all generators, and is a stabiliser of the states since $S_3S_4 = Z_5Z_6$, therefore we cannot detect that such an error happens, but it also does not affect our information
- Y_2Z_8 anticommutes with S_1 and S_7, thus we would identify there being a bit-flip on qubit 2, and a phase flip in the third block. However, in addition to the bit-flip on qubit 2 there is also a sign flip in this first block, but we have not detected it, since Y_2Z_8 commutes with S_8,

so only X_2X_7 and X_5Z_6 are correctable, but Z_5Z_6 does not alter our state.