Quantum Error Correction: Stabiliser Codes

IQC 2024 Lecture 28

Instructor: Joschka Roffe, joschka.roffe@ed.ac.uk

THE UNIVERSITY of EDINBURGH
informatics

Recap: The Challenges of Quantum Error Correction

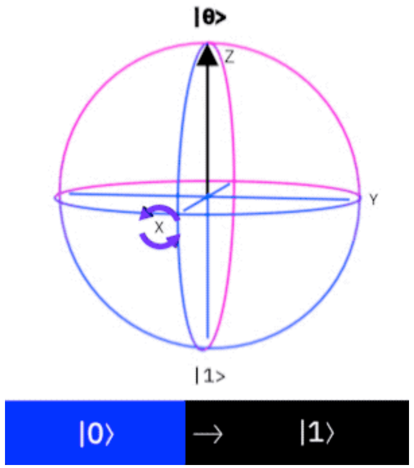
- **More complicated error channels**. In classical error correction we only need to worry about bit flips. In quantum error correction there are phase-flips too:

Bit flips: $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$

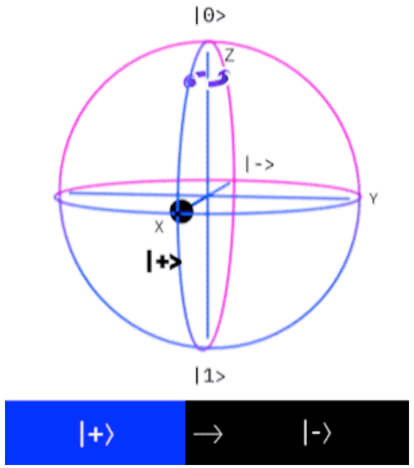
Phase flips: $Z|+\rangle = |-\rangle$ and $Z|-\rangle = |+\rangle$

- **The No-Cloning Theorem**: This prevents us from arbitrarily duplicating data as we do for classical repetition codes

- **Wavefunction collapse**: How do we check for errors in a quantum state without collapsing the encoded quantum information.



Evolution on the Bloch Sphere due to **bit-flip** (X-Pauli error)



Evolution on the Bloch Sphere due to **phase-flip** (Z-Pauli error)

THE UNIVERSITY of EDINBURGH
informatics

Recap: Subspace Encoding

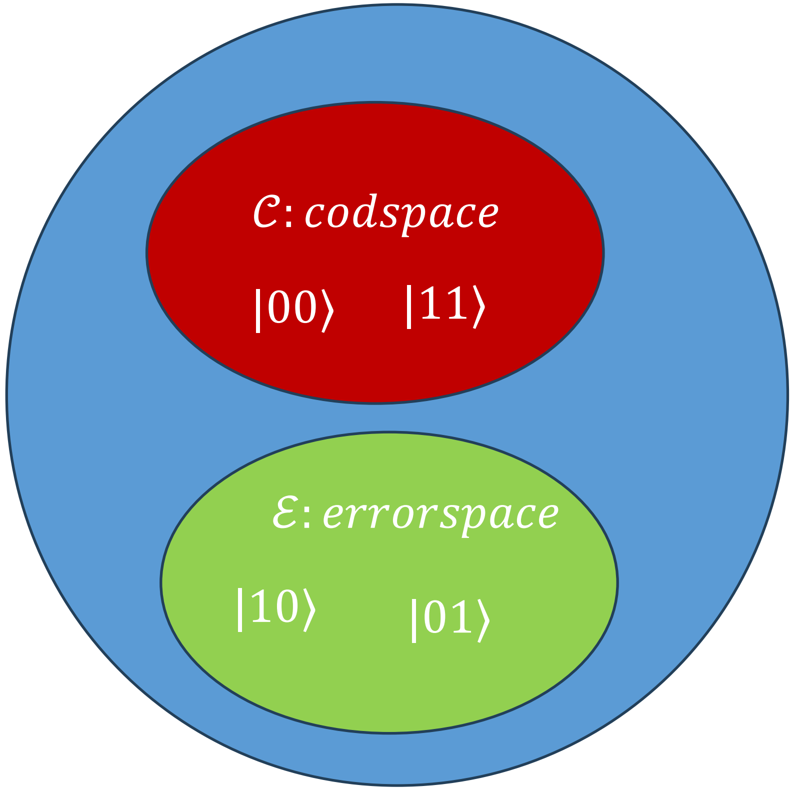
If the logical state is un-errored, it in the codespace

$$|\psi\rangle_L = (\alpha|00\rangle + \beta|11\rangle) \in \mathcal{C} \subset \mathcal{H}_4$$

If it is subject to a single-qubit Pauli-X error, the state is rotated into the error space. E.g.,

$$X_1|\psi\rangle_L = (\alpha|10\rangle + \beta|01\rangle) \in \mathcal{E} \subset \mathcal{H}_4$$

We can detect the occurrence of a single-qubit X-error by performing a measurement to determine which subspace the logical qubit is in.



Recap: Detecting errors via stabiliser measurement

The two-qubit code partitions the Hilbert space into a codespace and an errorspace:

The code-space: $\mathcal{C} = \text{span}(|00\rangle, |11\rangle)$

The error-space: $\mathcal{E} = \text{span}(|01\rangle, |10\rangle)$

We can differentiate between the codespace and the error space using a **Hadamard test** (recall Lecture 16). The projector onto the codespace is:

$$\Pi_{\mathcal{C}} = |00\rangle\langle 00| + |11\rangle\langle 11|$$

The projector on the errorspace is:

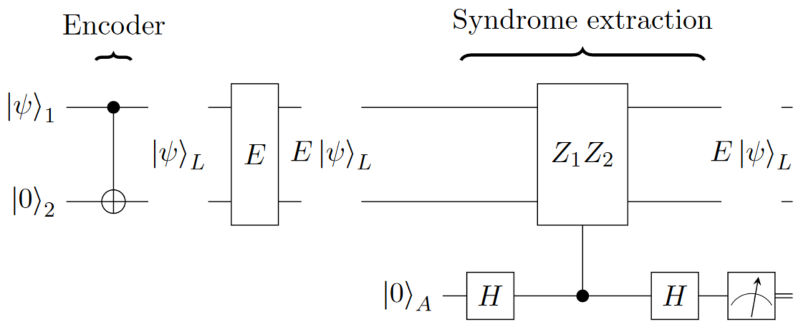
$$\Pi_{\mathcal{E}} = |01\rangle\langle 01| + |10\rangle\langle 10|$$

The following unitary operator has eigenvalues ± 1 depending upon whether it is applied to state in the codespace or the error space:

$$\Pi_S = \Pi_{\mathcal{C}} - \Pi_{\mathcal{E}} = Z_1 Z_2$$

The above operator is referred to as a **stabiliser** as it acts as the identity on the logical state:

$$Z_1 Z_2 |\psi\rangle_L = Z_1 Z_2(\alpha|00\rangle + \beta|11\rangle) = (+1)|\psi\rangle_L$$



The Hadamard test operator $Z_1 Z_1$ has ± 1 eigenvalues.

If the state is in the codespace, we measure the (+1) eigenvalue.

$$Z_1 Z_2 |\psi\rangle_L = Z_1 Z_2(\alpha|00\rangle + \beta|11\rangle) = (+1)|\psi\rangle_L$$

If the state is in the errorspace, we measure the (-1) eigenvalue.

$$Z_1 Z_2 (X_1|\psi\rangle_L) = Z_1 Z_2(\alpha|10\rangle + \beta|01\rangle) = (-1)E|\psi\rangle_L$$

This enables us to detect errors without destroying the superposition.

THE UNIVERSITY of EDINBURGH informatics

Recap: The [[4,2,2]] Detection Code

To detect both bit and phase-type errors, we require an encoding with stabilisers that anti-commute with both error types.

Example. The [4,2,2] code encodes two logical qubits in four physical qubits and has the following logical basis states

$$|00\rangle_L = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$$

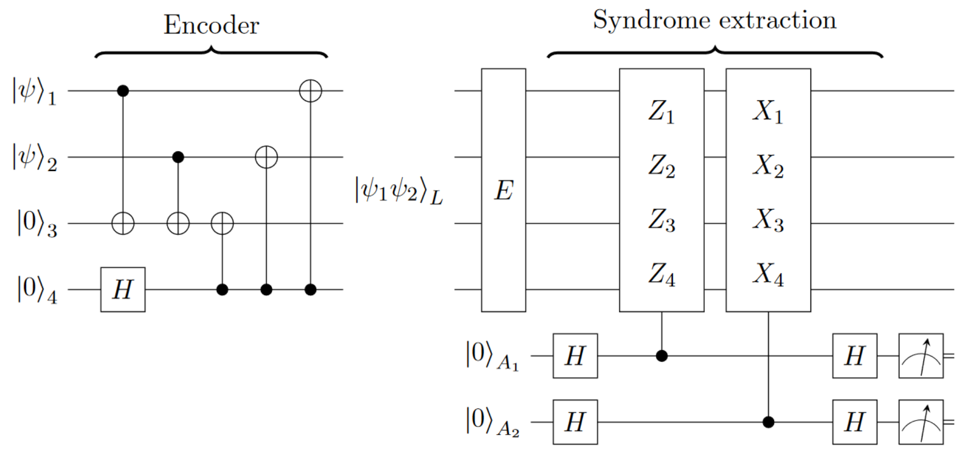
$$|01\rangle_L = \frac{1}{\sqrt{2}}(|1100\rangle + |0011\rangle)$$

$$|10\rangle_L = \frac{1}{\sqrt{2}}(|1010\rangle + |0101\rangle)$$

$$|11\rangle_L = \frac{1}{\sqrt{2}}(|0110\rangle + |1001\rangle)$$

The above basis states are simultaneously stabilised by the following generators:

$$X_1X_2X_3X_4$$
$$Z_1Z_2Z_3Z_4$$



Error	Syndrome, S	Error	Syndrome, S	Error	Syndrome, S
X_1	10	Z_1	01	Y_1	11
X_2	10	Z_2	01	Y_2	11
X_3	10	Z_3	01	Y_3	11
X_4	10	Z_4	01	Y_4	11

The syndrome table for the [4,2,2] detection code. Each single-qubit X/Y/Z error yields a non-zero syndrome. However, some syndromes are shared. -> This is a **detection** code not a **correction code**.

The Stabiliser Formalism for Quantum Error Correction

THE UNIVERSITY of EDINBURGH
informatics

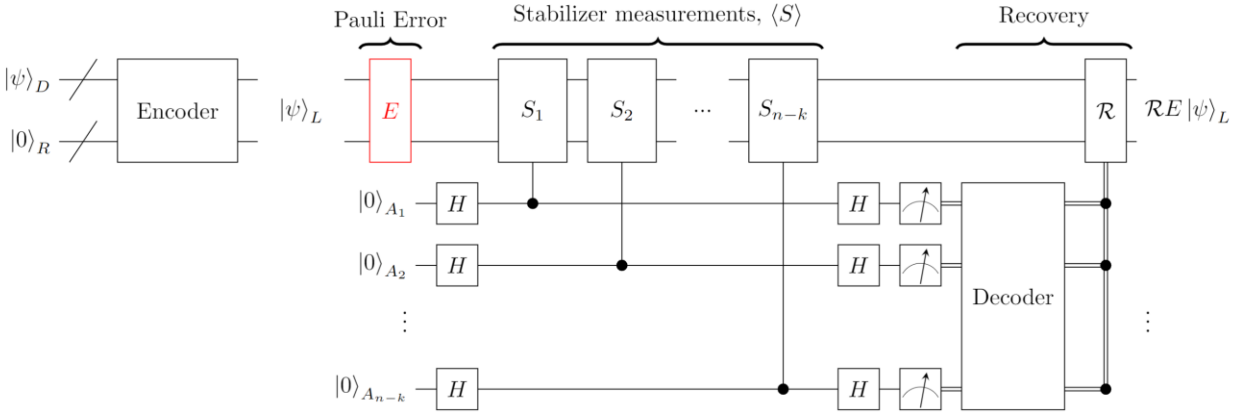
Stabiliser Codes

The Pauli Group: $\mathcal{P}^{\otimes n}$ is the Pauli-group $(\pm I, \pm iI, \pm X, \pm Y, \pm Z, \pm iX, \pm iY, \pm iZ)$ over n qubits. E.g., $X_1 I_2 Y_3 \in \mathcal{P}^{\otimes 3}$.

The stabilisers $\mathcal{S} \subset \mathcal{P}^{\otimes N}$ of a quantum error correction code simultaneously act as the identity on the logical state $|\psi\rangle_L$ such that:

$$G_i|\psi\rangle_L = (+1)|\psi\rangle_L \quad \text{for all} \quad G_i \in \mathcal{S}$$

To detect errors, a generating set $\langle S\rangle \subset \mathcal{S}$ is measured using the Hadamard test syndrome extraction gadgets (as described in Lecture 25).



Minimal generating set of stabilisers

A generating $\langle S\rangle$ in minimal if all operators in S are independent. E.g., $[Z_1Z_2,\ \ Z_2Z_3,\ Z_1Z_3]$ is not a generating set, as $Z_1Z_3 = (Z_1Z_2)(Z_2Z_3)$.

Stabiliser code syndromes

Measurement of generator S_i will yield outcome:

- $\mathrm{s_i} = 0$: if the error commutes with the generator, $[E, S_i] = 0$
- $\mathrm{s_i} = 1$: if the error anti-commutes with the generator, $\{\mathrm{E}, S_i\} = 0$

The **syndrome** is the binary string obtained by concatenating all of the generator measurement outcomes: $\mathrm{s} = \mathrm{s_1 s_2 \ldots s_m}$, where m is the size of the generating set, $m = |S|$.

THE UNIVERSITY of EDINBURGH informatics

The Stabiliser Group is Abelian

The stabiliser group is **abelian**: all elements of $\mathcal{S}$ mutually commute:

$$[G_i, G_j] = 0 \quad \text{for all} \quad G_i, G_j \in \mathcal{S}$$

Why?

Elements of $\mathcal{S}$ simultaneously stabilise the logical state such that

$$G_i G_j |\psi\rangle_L = (+1)(+1)|\psi\rangle_L \text{ for all } G_i, G_j \in \mathcal{S}$$

If $G_i G_j \in \mathcal{S}$ then we also have that $G_j G_i \in \mathcal{S}$.

This can only be true if $[G_i, G_j] = 0$ for all $G_i, G_j \in \mathcal{S}$.

Why (physicists edition)?

- The Heisenberg Uncertainty Principle stipulates that it is only possible to simultaneously measure **commuting** observables.
- Stabilisers are operators that are simultaneously measured on the logical state $|\psi\rangle_L$. Therefore, they must commute with one another.

Logical qubit count

The number of logical qubits k encoded by a stabiliser code is given by:

$$k = n - \text{rank}(\mathcal{S})$$

Where:

n: number of physical qubits

k: number of logical qubits

$\text{rank}(\mathcal{S})$: size of the minimal generating set $|S|$.

Example: The [[4,2,2]] code is defined by the following stabilisers:

$$\mathcal{S} = \langle S \rangle = \left\langle \begin{matrix} X_1 X_2 X_3 X_4 \\ Z_1 Z_2 Z_3 Z_4 \end{matrix} \right\rangle$$

S is a minimal generating set of size $|S|$= 2. The code is defined over $n = 4$ physical qubits. The number of logical qubits encoded is:

$$k = n - \text{rank}(\mathcal{S}) = n - |S| = 4 - 2 = 2$$

Properties of logical operators

We have seen that logical operators correspond to Pauli-operators L_i that act non-trivially on the basis states. E.g.

$$X_L|0\rangle_L = |1\rangle_L, \qquad X_L|1\rangle_L = |0\rangle_L$$

$$Z_L|0\rangle_L = |0\rangle_L, \qquad Z_L|1\rangle_L = (-1)|1\rangle_L$$

This means that any logical operator is **not** a stabiliser. We define a logical group $\mathcal{L} \subset \mathcal{P}^{\otimes n}$. The intersection with the stabiliser group is empty:

$$\mathcal{L} \cap \mathcal{S} = \emptyset$$

We have also seen that logical operators always map to the zero syndrome (they are undetectable). This means that any logical operator L_i must commute with all the stabilisers:

$$[L_i, G_j] = 0 \text{ for all } L_i \in \mathcal{L}, G_i \in \mathcal{S}$$

Every stabiliser code has $2k$ logical operators. For each logical qubit i there is:

- One X-type logical X_{L_i}
- One Z-type logical Z_{L_i}

We expect logical operator pairs X_{L_i}, Z_{L_i} to commute with one another:

$$\{X_{L_i}, Z_{L_i}\} = 0$$

THE UNIVERSITY of EDINBURGH informatics

Properties of Logical Operators Continued

Any logical operator multiplied by stabiliser is a logical operator:

$G_j L_i \in \mathcal{L}$ for all $L_i \in \mathcal{L}, G_i \in \mathcal{S}$.

Why?

Any logical operator L_i will commute with all the code stabilisers: $[L_i, G_j]$=0 for all $G_J \in \mathcal{S}$.

$$G_j L_i |\psi\rangle_L = L_i G_j |\psi\rangle_L$$

All stabilisers map onto the +1 eigenspace of $|\psi\rangle_L$:

$$L_i G_j |\psi\rangle_L = L_i |\psi\rangle_L$$

This means any product of $G_i L_j$ has logical action identical to that of L_j.

Example: Logical Operators of the [[4,2,2]] Code

Example: The [[4,2,2]] code is defined by the following stabilisers:

$$\mathcal{S} = \langle S \rangle = \left\langle \begin{matrix} X_1X_2X_3X_4 \\ Z_1Z_2Z_3Z_4 \end{matrix} \right\rangle$$

S is a minimal generating set of size |S|= 2. The code is defined over $n = 4$ physical qubits. The number of logical qubits encoded is:

$$k = n - |S| = 4 - 2 = 2$$

A basis of the logical operators is:

$$X_{L1} = X_1I_2X_3I_4, \quad Z_{L1} = Z_1Z_2I_3I_4$$
$$X_{L2} = X_1X_2I_2I_4, \quad Z_{L2} = Z_1I_2Z_3I_4$$

Non of the above can be obtained from a product of elements in $\mathcal{S}$.

We also see that $\{X_{Li}, Z_{Li}\}_+ = 0$ for both logical operator pairs

$$\{X_1I_2X_3I_4, Z_1Z_2I_3I_4\} = 0$$

$$\{X_1X_2I_2I_4, Z_1I_2Z_3I_4\} = 0$$

THE UNIVERSITY of EDINBURGH informatics

Designing Quantum Error Correction Codes

Error Detection Codes

Error detection codes have distance $d = 2$.

They can detect single-qubit Pauli errors but can't locate them.

Example: the [[4,2,2]] code is a detection code. See syndrome table below:

Error	Syndrome, S	Error	Syndrome, S	Error	Syndrome, S
X_1	10	Z_1	01	Y_1	11
X_2	10	Z_2	01	Y_2	11
X_3	10	Z_3	01	Y_3	11
X_4	10	Z_4	01	Y_4	11

Error Correction Codes

For a stabiliser code to be correcting, we need to be able to **detect** and **locate** errors.

The number of errors a code can correct t is give by:

$$t = \frac{d-1}{2}$$

By rearranging the above, we see that for a stabiliser code to be correcting it must have $d \geq 3$.

Example: The Steane Code

The Steane code is defined by the following stabiliser group generated by the stabilisers S:

$$\mathcal{S} = \langle S \rangle = \left\langle \begin{matrix} I_1\ I_2\ I_3\ X_4\ X_5\ X_6\ X_7 \\ I_1\ X_2\ X_3\ I_4\ I_5\ X_6\ X_7 \\ X_1\ I_2\ X_3\ I_4\ X_5\ I_6\ X_7 \\ I_1\ I_2\ I_3\ Z_4\ Z_5\ Z_6\ Z_7 \\ I_1\ I_2\ Z_3\ I_4\ I_5\ Z_6\ Z_7 \\ Z_1\ I_2\ Z_3\ I_4\ Z_5\ I_6\ Z_7 \end{matrix} \right\rangle$$

Number of logical qubits:

- The code is defined over 7 physical qubits: $n = 7$
- S is minimal generating set of size $|S| = 6$
- The number of logical qubits is:

$$k = n - \text{rank}(\mathcal{S}) = n - |S| = 7 - 6 = 1$$

Error (X)	Syndrome (s)	Error (Y)	Syndrome (s)	Error (Z)	Syndrome (s)
X_1	000001	Y_1	001001	Z_1	001000
X_2	000010	Y_2	010010	Z_2	010000
X_3	000011	Y_3	011011	Z_3	011000
X_4	000100	Y_4	100100	Z_4	100000
X_5	000101	Y_5	101101	Z_5	101000
X_6	000110	Y_6	110110	Z_6	110000
X_7	000111	Y_7	111111	Z_7	111000

Syndrome table:

Each single-qubit error maps to a unique syndrome.

This means that the distance of this code is at least $d = 3$. It is a **correction** code.

The Steane Code: Logical Operators

$$|0\rangle_L = \frac{1}{\sqrt{8}}[|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle]$$

$$|1\rangle_L = \frac{1}{\sqrt{8}}[|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle]$$

Logical operators

For the X-type logical operator X_L we need a Pauli-operator that acts as follows:

$$X_L|0\rangle_L = |1\rangle_L, \quad X_L|1\rangle_L = |0\rangle_L$$

For the Z-type logical operator Z_L, we need a Pauli-operator that acts as follows:

$$Z_L|0\rangle_L = |0\rangle_L, \quad Z_L|1\rangle_L = -|1\rangle_L$$

Steane Code: Logical basis

$$X_L = X_1X_2X_3X_4X_5X_6X_7$$

$$Z_L = Z_1Z_2Z_3Z_4Z_5Z_6Z_7$$

The above logical operators satisfy the anti-commutation relation: $\{X_L, Z_L\} = 0$.

Steane Code: Distance

Q: How do we know there isn't a logical operator with hamming weight <3?
A: From the syndrome table, we saw that all single-qubit errors have a unique syndrome, implying that this is an error correction code. All error correction codes must have distance $d \geq 3$.

The Steane code is defined by the following stabiliser group:

$$\mathcal{S} = \langle S \rangle = \left\langle \begin{matrix} I_1 I_2 I_3 X_4 X_5 X_6 X_7 \\ I_1 X_2 X_3 I_4 I_5 X_6 X_7 \\ X_1 I_2 X_3 I_4 X_5 I_6 X_7 \\ I_1 I_2 I_3 Z_4 Z_5 Z_6 Z_7 \\ I_1 I_2 Z_3 I_4 I_5 Z_6 Z_7 \\ Z_1 I_2 Z_3 I_4 Z_5 I_6 Z_7 \end{matrix} \right\rangle$$

A choice of logical operators are:

$$X_L = X_1 X_2 X_3 X_4 X_5 X_6 X_7$$

$$Z_L = Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 Z_7$$

The **code distance** is the minimum Hamming-weight of a logical operator. Both of the logical operators above have weight 7. However, we have to consider all logical operators in the group $\mathcal{L}$.

Any logical operator multiplied by a stabiliser is a logical operator: $G_i L_j \in \mathcal{S}$ for all $G_i \in \mathcal{S}$ and $L_j \in \mathcal{L}$.

If we multiply the X_L logical operator by the first stabiliser, we get another logical operator:

$$X_L' = (I_1 I_2 I_3 X_4 X_5 X_6 X_7)(X_1 X_2 X_3 X_4 X_5 X_6 X_7) = \mathrm{X}_1 \mathrm{X}_2 \mathrm{X}_3 \mathrm{I}_4 \mathrm{I}_5 \mathrm{I}_6 \mathrm{I}_7$$

Similarly, for the Z_L operator:

$$Z_L' = (I_1 I_2 I_3 Z_4 Z_5 Z_6 Z_7)(Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 Z_7) = Z_1 Z_2 Z_3 \mathrm{I}_4 \mathrm{I}_5 \mathrm{I}_6 \mathrm{I}_7$$

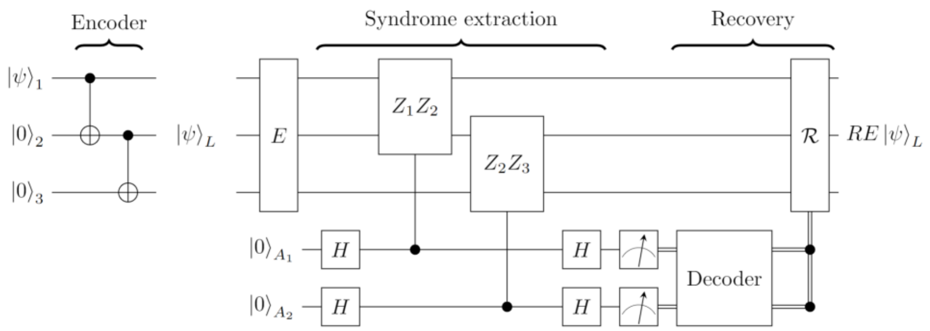
Both of the above logical operators have Hamming weight 3. The distance of the code is therefore $d = 3$.

The Steane code has node parameters: $[[n = 7, k = 1, d = 3]]$

The Shor Code: Code Construction by Concatenation

Code concatenation is a method of creating a larger code from two copies of a smaller code. The [[9,1,3]] code is a simple example that is obtained by concatenating a 3-bit repetition code for phase flips with a 3-qubit repition code for bit-flips.

3-qubit code for bit-flips



Stabilisers:

$$S^{3bit} = \langle Z_1Z_2, \quad Z_2Z_3\rangle$$

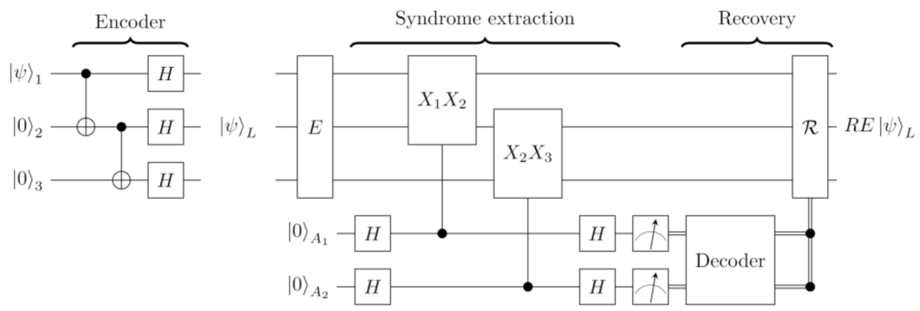
Basis states:

$$|0\rangle_L^{3bit} = |000\rangle, \quad |1\rangle_L^{3bit} = |111\rangle$$

Logical operators:

$$X_L^{3bit} = X_1X_2X_3, \quad Z_L^{3bit} = Z_1I_2I_3$$

3-qubit code for phase-flips



Stabilisers:

$$S^{3phase} = \langle X_1X_2, \quad X_2X_3\rangle$$

Basis states:

$$|0\rangle_L^{3phase} = |+++\rangle, \quad |1\rangle_L^{3phase} = |---\rangle$$

Logical operators:

$$X_L^{3phase} = Z_1Z_2Z_3, \quad Z_L^{3phase} = X_1I_2I_3$$

Shor Code: Encoding via Concatentation

Outer code encoding

$$|0\rangle_L^{outer} = |{+}{+}{+}\rangle, \quad |1\rangle_L^{inner} = |{-}{-}{-}\rangle$$

Inner code encoding: The basis states of the Shor code are obtained by replacing each qubit in the above with a logical qubit from the bit-flip code.

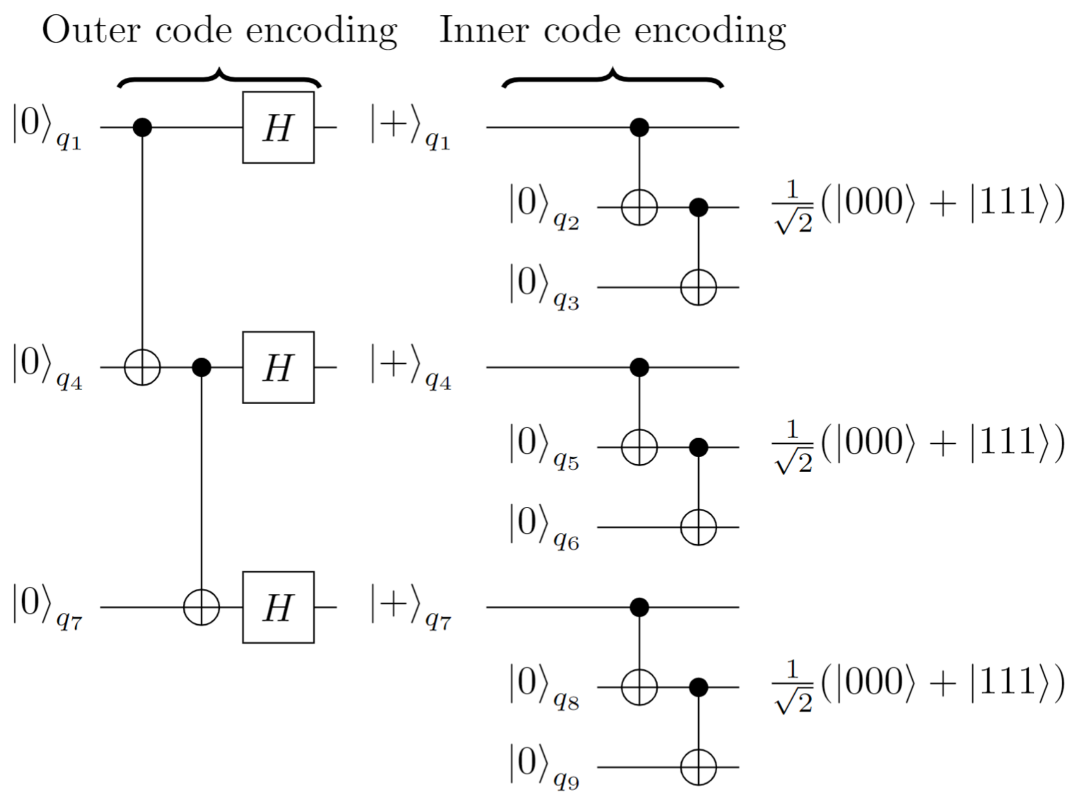
$$|0\rangle_L = \frac{1}{\sqrt{8}}(|0\rangle_L^{inner} + |1\rangle_L^{inner}) \otimes (|0\rangle_L^{inner} + |1\rangle_L^{inner}) \otimes (|0\rangle_L^{inner} + |1\rangle_L^{inner})$$

$$|1\rangle_L = \frac{1}{\sqrt{8}}(|0\rangle_L^{inner} - |1\rangle_L^{inner}) \otimes (|0\rangle_L^{inner} - |1\rangle_L^{inner}) \otimes (|0\rangle_L^{inner} - |1\rangle_L^{inner})$$

This expands to:

$$|0\rangle_L = \frac{1}{\sqrt{8}}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$|1\rangle_L = \frac{1}{\sqrt{8}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$



THE UNIVERSITY of EDINBURGH informatics

Shor Code Stabilisers

From inner bit-flip code, we get three sets of two stabilisers:

$$\begin{matrix} Z_1Z_2, & Z_2Z_3 \\ Z_4Z_5, & Z_5Z_6 \\ Z_7Z_8, & Z_8Z_9 \end{matrix}$$

We get an additional two stabiliser from the outer code.

The outer code stabilisers are: $S_1^{outer} = XXI,\ S_2^{outer} = IXX$

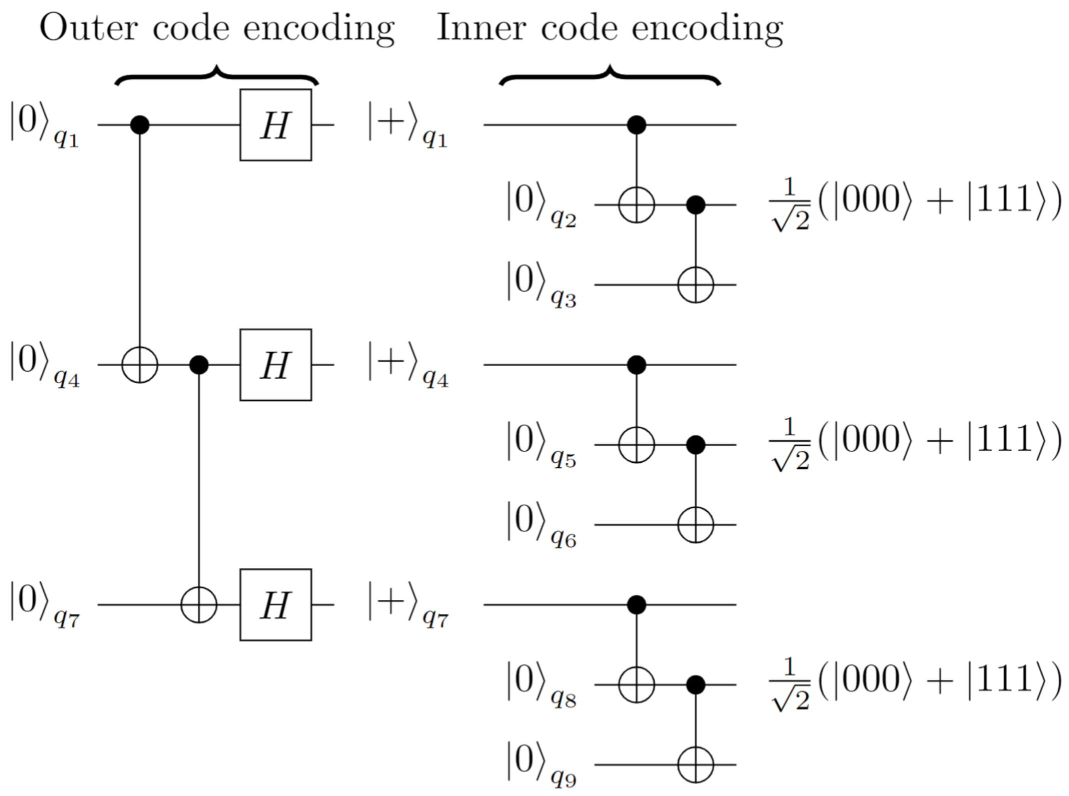
We replace each Pauli from the outer code with a logical Pauli from the inner code:

$$XXI \rightarrow (X_{L1}^{inner}) \otimes (X_{L2}^{inner}) \otimes (I_L^{inner})$$

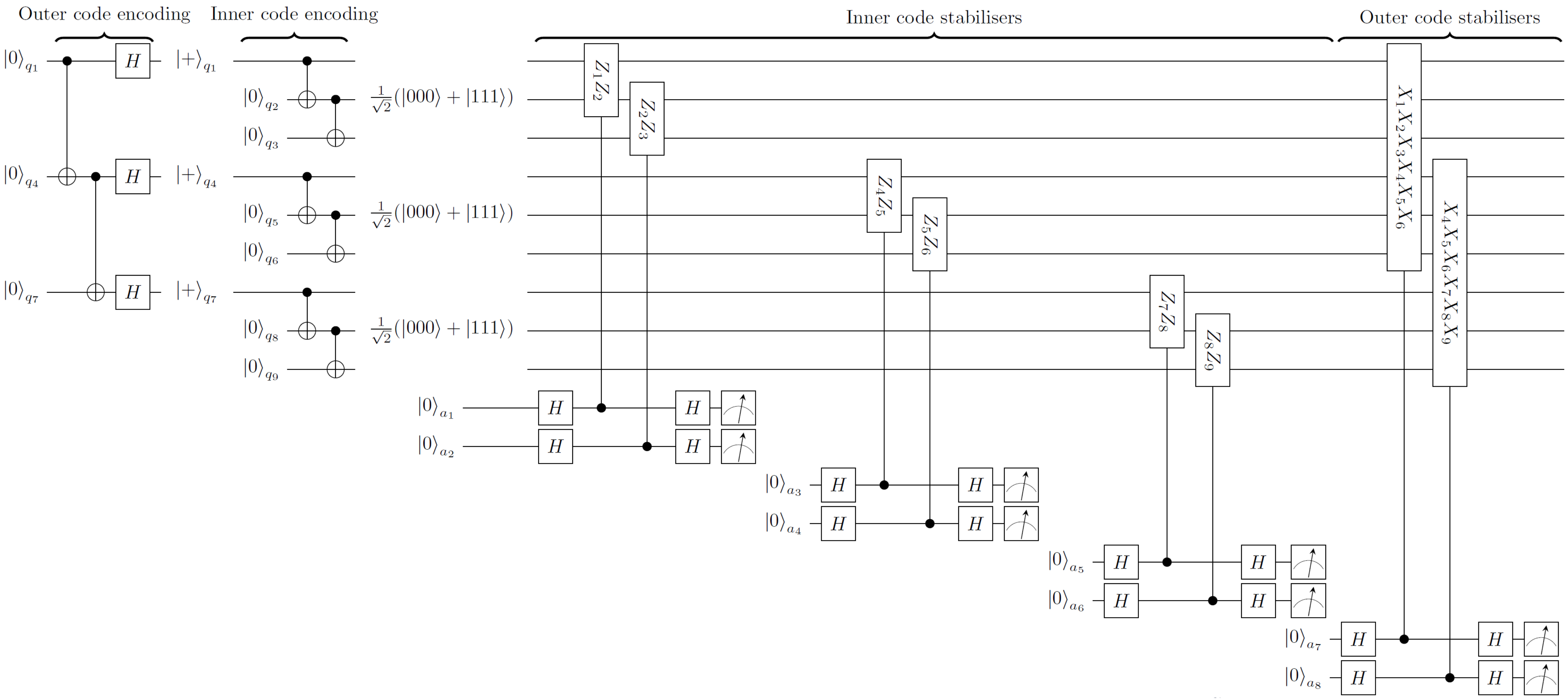
$$= (X_1X_2X_3) \otimes (X_4X_5X_6) \otimes (I_7I_8I_9) = X_1X_2X_3X_4X_5X_6I_7I_8I_9$$

$$IXX \rightarrow (I_L^{inner}) \otimes (X_{L2}^{inner}) \otimes (X_{L3}^{inner})$$

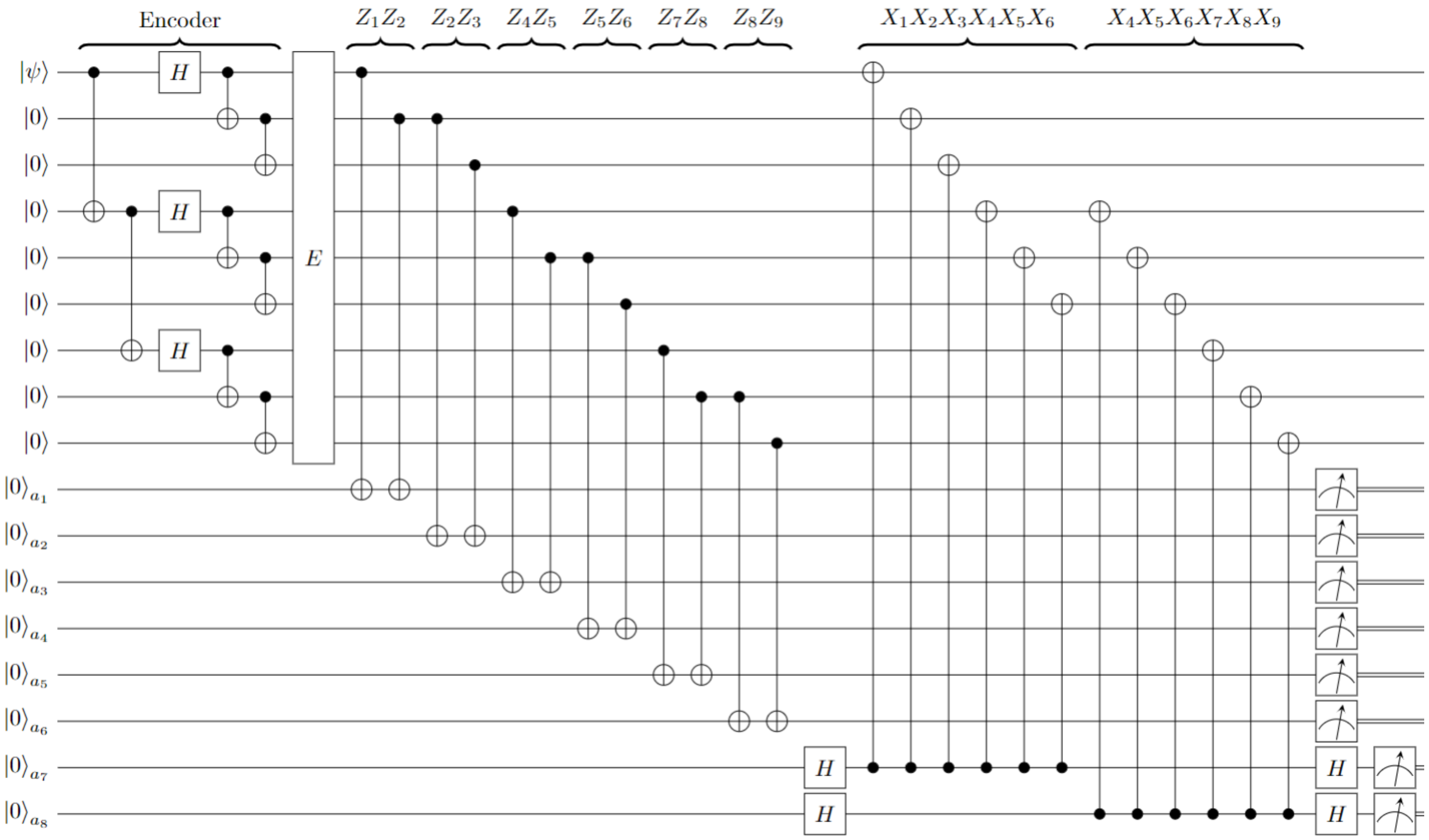
$$= (I_1I_2I_3) \otimes (X_4X_5X_6) \otimes (X_7X_8X_9) = I_1I_2I_3X_4X_5X_6X_7X_8X_9$$



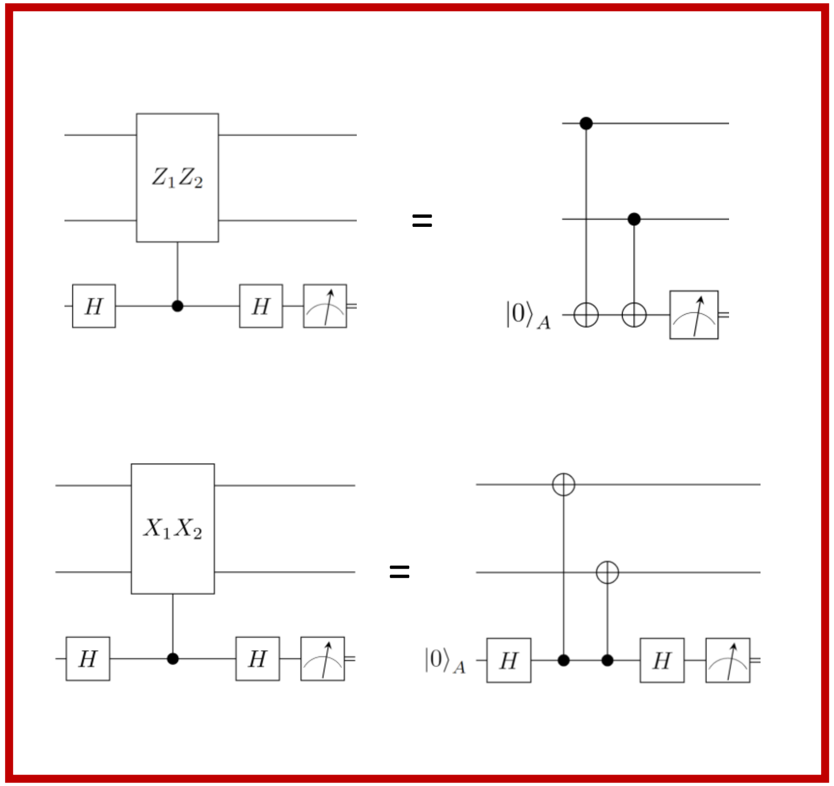
Shor Code Stabilisers



Shor [[9,1,3]] Code Circuit



Compiling stabiliser checks with CNOT gates



THE UNIVERSITY of EDINBURGH informatics

Shor Code: Logical Operators and Distance

$$|0\rangle_L = \frac{1}{\sqrt{8}}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$|1\rangle_L = \frac{1}{\sqrt{8}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$

Outer code logical operators:

$$X_L^{outer} = ZZZ$$
$$Z_L^{outer} = XII$$

Inner code logical operators:

$$X_L^{inner} = XXX$$
$$Z_L^{inner} = ZII$$

To get the Shor code logical operators, we replace each Pauli in the outer code with a logical Pauli from the inner code

$$Z_L^{outer} = XII \quad \rightarrow \quad X_L^{inner} \otimes I_L^{inner} \otimes I_L^{inner} = X_1X_2X_3I_4I_5I_6I_7I_8I_9$$

$$X_L^{outer} = ZZZ \quad \rightarrow (Z_L^{inner}) \otimes (Z_L^{inner}) \otimes (Z_L^{inner}) = Z_1I_2I_3Z_4I_5I_6Z_7I_8I_9$$

The Shor Code Logical operators are:

$X_L = Z_1I_2I_3Z_4I_5I_6Z_7I_8I_9\,, \quad Z_L = X_1X_2X_3I_4I_5I_6I_7I_8I_9$

The Shor Code has distance $d = 3$

THE UNIVERSITY of EDINBURGH informatics

Shor Code: [[n,k,d]] Parameters

Stabiliser generators

$$\langle S \rangle = \left\langle \begin{matrix} Z_1 Z_2 I_3 I_4 I_5 I_6 I_7 I_8 I_9 \\ I_1 Z_2 Z_3 I_4 I_5 I_6 I_7 I_8 I_9 \\ I_1 I_2 I_3 Z_4 Z_5 I_6 I_7 I_8 I_9 \\ I_1 I_2 I_3 I_4 Z_5 Z_6 I_7 I_8 I_9 \\ I_1 I_2 I_3 I_4 I_5 I_6 Z_7 Z_8 I_9 \\ I_1 I_2 I_3 I_4 I_5 I_6 I_7 Z_8 Z_9 \\ X_1 X_2 X_3 X_4 X_5 X_6 I_7 I_8 I_9 \\ I_1 I_2 I_3 X_4 X_5 X_6 X_7 X_8 X_9 \end{matrix} \right\rangle$$

Logical qubit count

$k = n - |S|$

Physical qubits, $n = 9$

S is a minimal generating set of size $|S| = 8$

The logical qubit count is

$$k = 9 - 8 = 1$$

Code distance

d=3 (see previous slide)

Code parameters

[[n=9, k=1, d=3]]

THE UNIVERSITY of EDINBURGH informatics

Shor Code: Syndrome Table & Degenerate Errors

Error (X)	Syndrome (s)	Error (Y)	Syndrome (s)	Error (Z)	Syndrome (s)
X_1	10000000	Y_1	10000010	Z_1	00000010
X_2	11000000	Y_2	11000010	Z_2	00000010
X_3	01000000	Y_3	01000010	Z_3	00000010
X_4	00100000	Y_4	00100011	Z_4	00000011
X_5	00110000	Y_5	00110011	Z_5	00000011
X_6	00010000	Y_6	00010011	Z_6	00000011
X_7	00001000	Y_7	00001001	Z_7	00000001
X_8	00011000	Y_8	00011001	Z_8	00000001
X_9	00000100	Y_9	00000101	Z_9	00000001

Shor Code stabiliser generators:

$$\langle S\rangle = \left\langle \begin{array}{ccccccccc} Z_1 & Z_2 & I_3 & I_4 & I_5 & I_6 & I_7 & I_8 & I_9 \\ I_1 & Z_2 & Z_3 & I_4 & I_5 & I_6 & I_7 & I_8 & I_9 \\ I_1 & I_2 & I_3 & Z_4 & Z_5 & I_6 & I_7 & I_8 & I_9 \\ I_1 & I_2 & I_3 & I_4 & Z_5 & Z_6 & I_7 & I_8 & I_9 \\ I_1 & I_2 & I_3 & I_4 & I_5 & I_6 & Z_7 & Z_8 & I_9 \\ I_1 & I_2 & I_3 & I_4 & I_5 & I_6 & I_7 & Z_8 & Z_9 \\ X_1 & X_2 & X_3 & X_4 & X_5 & X_6 & I_7 & I_8 & I_9 \\ I_1 & I_2 & I_3 & X_4 & X_5 & X_6 & X_7 & X_8 & X_9 \end{array} \right\rangle$$

Note that some of the Z-errors share a syndrome.

Q: Does this mean the Shor code is a detection code?

A: No. Consider the scenario in which the error $\mathrm{E} = Z_1$ occurs. This error shares syndromes with Z_2 and Z_3. Therefore, our decoder must choose Z_1, Z_2 or Z_3 at random:

- If recovery $R = Z_1$, then $RE = I \in \mathcal{S}$
- If recovery $R = Z_2$, then $RE = Z_1 Z_2 \in \mathcal{S}$
- If recovery $R = Z_3$, then $RE = \mathrm{Z}_1 \mathrm{Z}_3 \in \mathcal{S}$

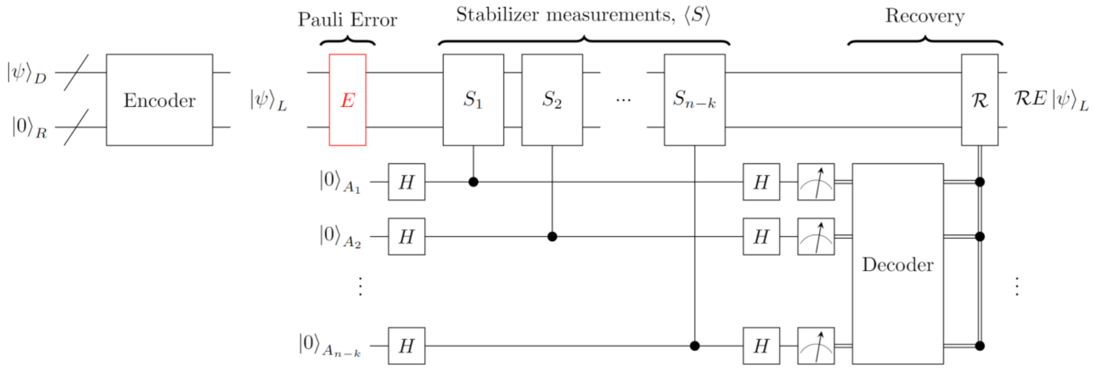
In all three scenarios, the residual error $RE \in \mathcal{S}$. Therefore, it doesn't matter which correction we choose and the Shor code is still a correction code.

Errors of the same Hamming weight that share syndromes are called **degenerate errors**.

Unique syndromes are a sufficient condition for a code to be correcting, but not necessary.

THE UNIVERSITY of EDINBURGH informatics

The Error Correction Cycle



The error correction cycle

1. Encoder: creates the logical state $|\psi\rangle_L$
2. Stabiliser measurements: error detected by measuring stabiliser generators $S_i \in S$ yielding a binary syndrome s.
3. A decoding algorithm (run a classical co-processor) interprets the syndrome and suggests a recovery operation $\mathcal{R}$.
4. The recovery operation is applied to the register.

Determining QEC success

At the end of the cycle, we are left with the state $\mathcal{R}E|\psi\rangle_L$. We refer to $\mathcal{R}E$ as the residual error.

- **Successful QEC**: If $\mathcal{R}E \in \mathcal{S}$ then the QEC cycle has been successful as the residual is equal to a stabiliser:

$$\mathcal{R}E|\psi\rangle_L = (+1)|\psi\rangle_L.$$

- **Unsuccessful QEC**: If $\mathcal{R}E \in \mathcal{L}$ then the encoded information is modified and the QEC procedure has failed.

THE UNIVERSITY of EDINBURGH informatics

Encoding circuits

The $|0\rangle_L$ codeword for any [[n,k,d]] stabiliser code can be obtained via a projection onto the $+1$ eigenspace of all of the stabilisers generators $S_i \in S$:

$$|0\rangle_L = \frac{1}{N} \prod_{S_i \in \langle S \rangle} (I + S_i) \, |0^{\otimes n}\rangle$$

where the $1/N$ term is a factor that ensures normalisation.

- This operator is non-unitary.
- However, it can be prepared by measuring all of the stabilisers on the blank $|0^{\otimes n}\rangle$ state.

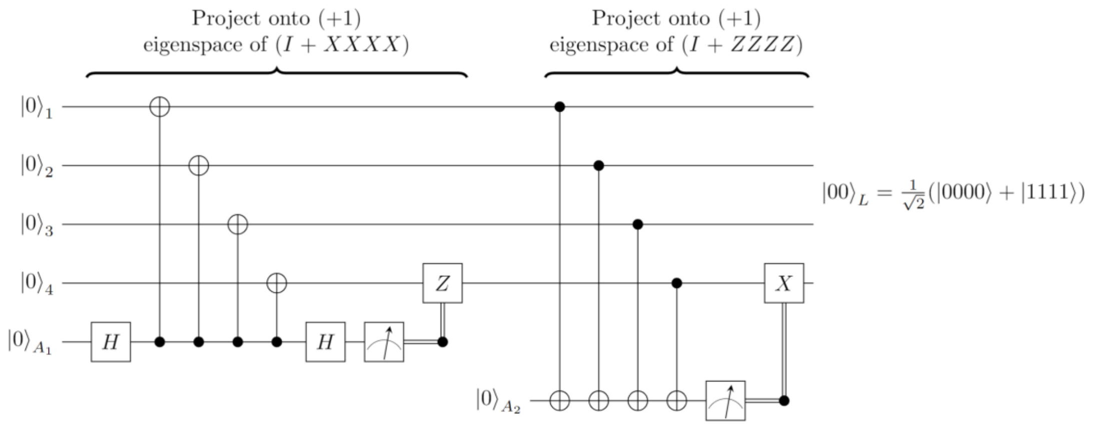
[[4,2,2]] Code Encoding Circuit

Immediately before the measurement of A_1, the system is in the state:

$$\frac{1}{2}(1 + X_1X_2X_3X_4)|0000\rangle|0\rangle_{A_1} + \frac{1}{2}(1 - X_1X_2X_3X_4)|0000\rangle|1\rangle_{A_1}$$

- If A_1 is measured as `0', then we have projected onto the +1 eigenspace.
- If A_2 is measured as `1' then we are in the (-1) eigenspace. We can rotate into the correct subspace by applying any operator to the register that anti-commutes with $XXXX$.

For the $Z_1Z_2Z_3Z_4$ stabiliser, no correction is necessary as it stabilises both $|0000\rangle$ and $|1111\rangle$.



THE UNIVERSITY of EDINBURGH informatics

THE UNIVERSITY *of* EDINBURGH

informatics

www.informatics.ed.ac.uk