

Introduction to Quantum Error Correction

IQC 2024 Lecture 25

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





Quantum gate error rates

Median Fidelity (per op.)

99.9%

98.5%

Single-qubit gates Two-qubit gates (ISWAP)

FROM \$900K USD

NOVERA



QuEra Aquila: 256 qubit neutral-atom quantum computer [1]

Two-qubit gate fidelity: **99.5%** [2]

[1] <u>https://quera.com</u>

[2] <u>Nature</u> volume 622, pages 268–272 (2023) Rigetti Novera superconducting qubit quantum computer [4]

[3] https://www.rigetti.com/novera





Classical vs. Quantum Computing

- Transitor gates in classical CPUs are extremely robust.
- Failure rates $p \ll 1 \times 10^{-15}$ [Shivakumar et al. 2002].
- Classical gates are over a **trillion** times more reliable than qubit gates!

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you. 9% complete For more information about this issue and possible fixes, visit https://www.windows. top code: DRIVER_IRQL_NOT_LESS_OR_EQUAL The dreaded "Blue Screen of Death". Faults such as these are due



to software errors rather than hardware in classical CPUs.



Quantum Error Correction

Quantum error correction describes a family of system-level techniques that allow quantum computers to be built **fault-tolerantly** using noisy qubits.

Interviewer: It says here you're extremely fast at factoring, what are the factors of 9025?

Quantum computer: 7 and 11.

Interviewer: that's not even close

Quantum computer: yeah, but it was fast.







Classical error correction

• Raw binary encodings have **zero** redundancy. E.g.

bin(42) →101010

• Applying a single bit flip to our binary encoding completely changes its meaning.

dec(100010)=34

• How do we make our encoding more fault tolerant?



The Classical Repetition Code

In repetition code protocols redundancy is introduced by duplicating each bit. E.g. applying the 3-bit repetition code protocol to our binary encoding gives:

 $101010 \rightarrow (111)(000)(111)(000)(111)(000)$

We can now detect and correct single-bit faults through a majority vote:

 $(101)(100)(011)(000)(111)(010) \rightarrow$

(111)(000)(111)(000)(111)(000)



The Classical Repetition Code

3-bit repetition code. Binary symbols mapped to 3-bit codewords.

 $\{0,1\} \to \{000,111\}$

- Single-bit errors can be corrected via majority vote. E.g., $000 \rightarrow 010 \rightarrow 000$
- Two-bit errors can be detected, but are incorrectly corrected via majority vote. E.g. $000 \rightarrow 011 \rightarrow 111$
- Three-bit errors are undetectable via majority vote: 000 → 111

Code distance: The code distance is the minimum Hamming-weight of an undetectable error. E.g., distance d=3 for the 3-bit repetition code.

An error correction code can correct *t* errors, where:

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

[n,k,d] Notation

n: codeword length

k: encoded message length

d: code distance

E.g. 3-bit repetition code has parameters: [n = 3, k = 1, d = 3]



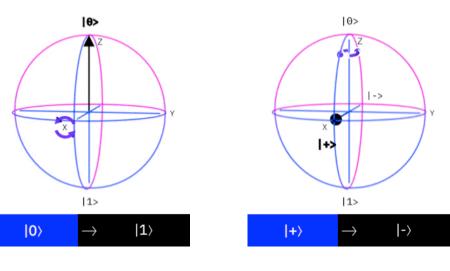


The Challenges of Quantum Error Correction

• 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 **phaseflip** (Z-Pauli error)





The No-Cloning Theorem

Q: Can we create a quantum repetition code by duplicating states?

 $|\psi\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle.$

A: No! This is prohibited by the No-Cloning Theorem.



Dolly would not have existed had she been a Quantum Sheep. Image source: National Museum of Scotland

No-Cloning Theorem Derivation

For cloning, we require a unitary *U* that duplicates quantum information as follows:

 $U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle.$

The cloning unitary should apply to any state:

 $U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$ $U(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle$

Unitary operation preserve the inner product. Taking the inner product of the above gives:

• There are only two solutions to the above. Either:

 $|\psi\rangle = |\phi\rangle$ or $\langle\psi|\phi\rangle = 0$

- Therefore, *U* only exists for states that are orthogonal.
- There is no unitary *U* that can clone arbitrary states.



The two-bit repetition code: redundancy without cloning

The two-qubit repetition code

We can circumvent the No-Cloning theorem and redundantly encode quantum information using *entanglement*.

The two-qubit repetition code maps the computational basis $\{|0\rangle, |1\rangle\}$, to the **Logical basis states:**

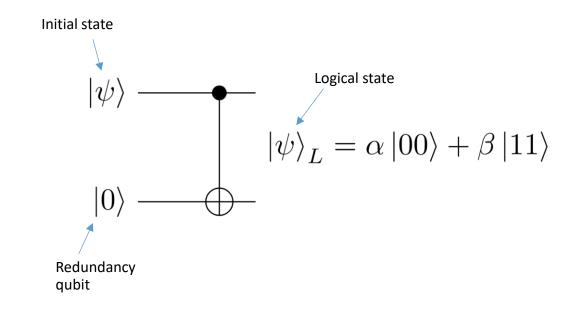
 $|0\rangle_L = |00\rangle$ and $|1\rangle_L = |11\rangle$

Example: Consider the following qubit state.

 $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$

The two-qubit repetition encoder creates the following **state**:

 $|\psi\rangle_L = \alpha |00\rangle + \beta |11\rangle$



Note. This is not cloning: $|\psi\rangle_L \neq |\psi\rangle \otimes |\psi\rangle$





The two-bit repetition code: partitioning the Hilbert space

Partitioning the Hilbert Space

Prior to encoding, the initial state *exists* within a two-dimensional Hilbert space.

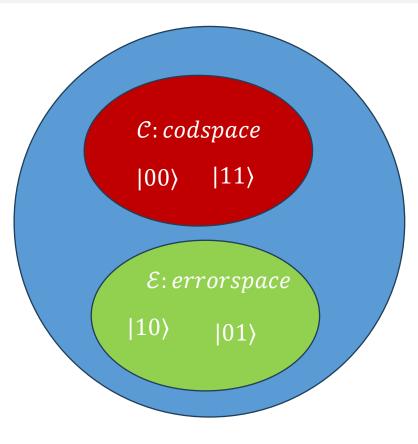
 $|\psi\rangle = (\alpha|0\rangle + \beta|1\rangle) \in \mathcal{H}_2 = \operatorname{span}(|0\rangle, |1\rangle)$

After encoding, the logical state exists within a four-dimensional Hilbert space:

 $|\psi\rangle_L = (\alpha|00\rangle + \beta|11\rangle) \in \mathcal{H}_4 = \operatorname{span}(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$

We can partition \mathcal{H}_4 into two orthogonal subspaces

- The code-space: $C = \text{span}(|00\rangle, |11\rangle)$
- The error-space: $\mathcal{E} = \text{span}(|01\rangle, |10\rangle)$





Errors map $\mathcal{C} \to \mathcal{E}$

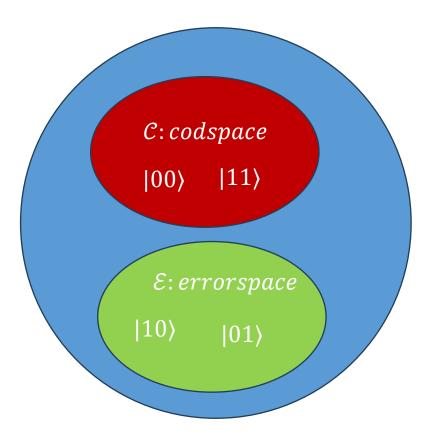
If the logical state is un-errored, it in the codespace

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

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 Xerror by performing a measurement to determine which subspace the logical qubit is in.





Detecting errors via stabiliser measurement

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

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

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:

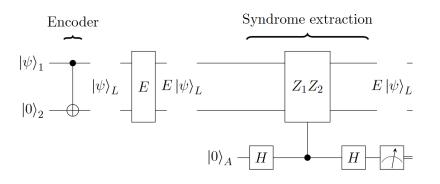
 $\Pi_{\mathcal{E}} = |01\rangle\langle 01| + |10\rangle\langle 10|$

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

$$\Pi_{\rm S} = \Pi_{\mathcal{C}} - \Pi_{\mathcal{E}} = \mathbf{Z}_1 \mathbf{Z}_2$$

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_1Z_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.





Error detection in the 2-qubit code

- **1.** Initial circuit state: $|\psi\rangle_1|0\rangle_2|0\rangle_A$
- **2.** After encoding: $|\psi\rangle_L|0\rangle_A$
- 3. Two qubit state after the Hadamard test (immediately before measurement of qubit A):

$$\frac{1}{2}(I+Z_1Z_2)\mathbf{E}|\psi\rangle_L|0\rangle_A+\frac{1}{2}(I-Z_1Z_2)\mathbf{E}|\psi\rangle_L|1\rangle_A$$

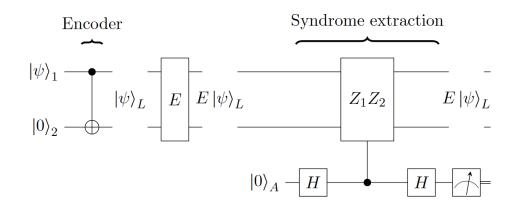
Examples

• If $E = I_1 I_2$ (no error case) we measure the `0` syndrome.

$$\frac{1}{2}(I + Z_1 Z_2)I_1 I_2 |\psi\rangle_L |0\rangle_A + \frac{1}{2}(I - Z_1 Z_2)I_1 I_2 |\psi\rangle_L |1\rangle_A$$
$$= \frac{1}{2}(I + Z_1 Z_2)I_1 I_2 |\psi\rangle_L |0\rangle_A = |\psi\rangle_L |0\rangle_A$$

• If $E = X_1 I_2$ we measure the `1` syndrome.

$$\frac{1}{2}(I + Z_1 Z_2) X_1 I_2 |\psi\rangle_L |0\rangle_A + \frac{1}{2}(I - Z_1 Z_2) X_1 I_2 |\psi\rangle_L |1\rangle_A$$
$$= \frac{1}{2}(I - Z_1 Z_2) X_1 I_2 |\psi\rangle_L |1\rangle_A = |\psi\rangle_L |1\rangle_A$$



- **1.** Encoder. Maps state $|\psi\rangle$ to the logical state $|\psi\rangle_L$.
- **2.** Error channel: we assume that the two-qubit state is subject to some Pauli-X error in the region marked by the gate *E*
- **3.** Stabiliser measurement and syndrome extraction. A Hadamard test can be performed to measure the operator Z_1Z_2 and determine whether an error has occurred. The binary outcome of the measurement on auxiliary qubit A is called the *syndrome*.



Error detection in the 2-qubit code

Pauli-operator commutation: Any pair of Pauli operators P_i , P_j either commute or anticommute with one another $[P_i, P_j] = 0$ or $\{P_i, P_j\} = 0$.

- **1.** After encoding: $|\psi\rangle_L |0\rangle_A$
- 2. After the Hadamard test (immediately before measurement of qubit A):

$$\frac{1}{2}(I+Z_1Z_2)\mathbf{E}|\psi\rangle_L|0\rangle_A+\frac{1}{2}(I-Z_1Z_2)\mathbf{E}|\psi\rangle_L|1\rangle_A$$

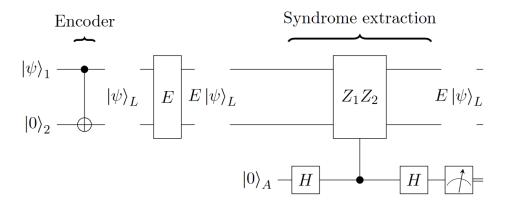
Assume that *E* is a Pauli operator.

If error commutes with stabiliser, $[E, Z_1Z_2] = 0$, then we are in the codespace and we measure the `0` syndrome.

$$\frac{1}{2}(I + Z_1 Z_2)E|\psi\rangle_L|0\rangle_A + \frac{1}{2}(I - Z_1 Z_2)E|\psi\rangle_L|1\rangle_A$$
$$= \frac{1}{2}E(I + Z_1 Z_2)|\psi\rangle_L|0\rangle_A + \frac{1}{2}E(I - Z_1 Z_2)|\psi\rangle_L|1\rangle_A = E|\psi\rangle_L|0\rangle_A$$

If error anti-commutes with the stabiliser, $\{E, Z_1Z_2\} = 0$, then we are in the the errorspace and we measure the `1` syndrome.

$$\begin{aligned} &\frac{1}{2}(I+Z_1Z_2)E|\psi\rangle_L|0\rangle_A + \frac{1}{2}(I-Z_1Z_2)E|\psi\rangle_L|1\rangle_A \\ &= \frac{1}{2}E(I+Z_1Z_2)|\psi\rangle_L|0\rangle_A + \frac{1}{2}E(I-Z_1Z_2)|\psi\rangle_L|1\rangle_A = E|\psi\rangle_L|1\rangle_A \end{aligned}$$



Pauli Error, E	Syndrome readout, A
$I_1 \otimes I_2$	0
$X_1 \otimes I_2$	1
$I_1 \otimes X_2$	1
$X_1 \otimes X_2$	0

The syndrome measurement A depends upon whether the error E commutes or anti-comutes with the stabiliser Z_1Z_2





Pauli commutation rules

All single qubit Pauli operators X, Y, Z anti-commute with one another.

 $\begin{array}{l} X_1 Z_1 = -Z_1 X_1 \\ X_1 Y_1 = -Y_1 X_1 \\ Z_1 Y_1 = -Y_1 Z_1 \end{array}$

Multi-qubit Pauli operators anticommute if they **non-trivially intersect** on an odd number of qubits.

An intersection is *trivial* if a Pauli operator of type $\lambda \in (X, Y, Z)$ intersects with another Pauli of type Lambda or the identity. **Example 1**: X_1Z_2 and Z_1Z_2

- Non-trivially intersect on qubit 1: Anti-commute.

Example 2: X_1I_2 and I_1Z_2

- Do not intersect: Commute.

Example 3: Z_1X_2 and X_1Z_2

- Non-trivially intersect on qubits 1 and 2. Even number of non-trivial intersections: *Commute*

Example 4: $Z_1I_2Z_3Y_4$ and $X_1X_2X_3X_4$.

- Non-trivially intersect on qubits 1, 3 and 4. Odd number of intersections: *Anti-commute.*

Example 5: $Z_1X_2I_3$ and $Z_1I_2X_3$

- All intersections are trivial: commute.



the university of edinburgh informatics

The three-qubit repetition code

To detect **and** correct errors, we require a larger Hilbert space and multiple overlapping stabiliser measurements. E.g. the three-bit repetition code:

$$|\psi\rangle_L = \alpha |000\rangle + \beta |111\rangle$$

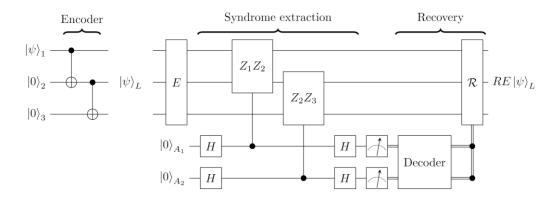
with logical basis states:

 $|0\rangle_L = |000\rangle, \qquad |1\rangle_L = |111\rangle$

This code has two independent stabilisers: Z_1Z_2 and Z_2Z_3

 $Z_1 Z_2 |00\rangle_L = |00\rangle_L$ and $Z_1 Z_2 |11\rangle_L = |11\rangle_L$ $Z_2 Z_3 |00\rangle_L = |00\rangle_L$ and $Z_2 Z_3 |11\rangle_L = |11\rangle_L$

Each single-qubit X-error maps to a unique syndrome. The three-qubit code is therefore a **correction** code (the two-qubit code is a detection code). Recovery operations can be applied by consulting a look-up table.



Pauli Error, E	Syndrome readout, A_1A_2	Recovery operation	
$I_1 \otimes I_2 \otimes I_3$	00	$I_1 \otimes I_2 \otimes I_3$	
$I_1 \otimes I_2 \otimes X_3$	01	$I_1 \otimes I_2 \otimes X_3$	
$I_1 \otimes X_2 \otimes I_3$	11	$I_1 \otimes X_2 \otimes I_3$	
$X_1 \otimes I_2 \otimes I_3$	10	$X_1 \otimes I_2 \otimes I_3$	
$I_1 \otimes X_2 \otimes X_3$	10	$I_1 \otimes X_2 \otimes X_3$	
$X_1 \otimes X_2 \otimes I_3$	01	$X_1 \otimes X_2 \otimes I_3$	
$X_1 \otimes I_2 \otimes X_3$	11	$X_1 \otimes I_2 \otimes X_3$	

The digitisation of the error

So far, we've only considered Pauli-X type errors. We now consider the other error types qubits can be subject to.

A general qubit state can be represented as point on a Bloch sphere

 $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$

Coherent errors can be described a unitary that rotates the state from one point on the Bloch sphere to another:

$$U(\delta\theta,\delta\phi)|\psi\rangle = \cos\left(\frac{\theta+\delta\theta}{2}\right)|0\rangle + e^{i(\phi+\delta\phi)}sin\left(\frac{\theta+\delta\theta}{2}\right)|1\rangle$$

In classical error correction, we only need to worry about one type of error: bit-flips. For qubits, we have an infinite number of errors $U(\delta\theta, \delta\phi)$ corresponding to arbitrary rotations around the Bloch sphere.

This is problematic, as error correction is not generally possible for analogue encodings

Q: Is error correction still possible?

A: Yes!

The coherent error $U(\delta\theta, \delta\phi)$ is a unitary 2x2 matrix.

Any 2x2 matrix can be expanded in terms of a Pauli basis $\{I, X, Z, Y\}$.

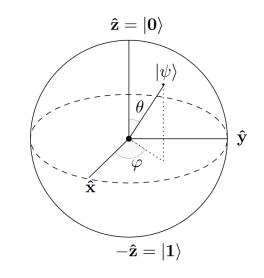
 $U(\delta\theta, \delta\phi)|\psi\rangle = \alpha_I |\psi\rangle + \alpha_X X |\psi\rangle + \alpha_Y Y |\psi\rangle + \alpha_Z Z |\psi\rangle$

Recall that $Y \propto XZ$. The above can therefore be written.

 $U(\delta\theta, \delta\phi)|\psi\rangle = \alpha_I |\psi\rangle + \alpha_X X |\psi\rangle + \alpha_{XZ} X Z |\psi\rangle + \alpha_Z Z |\psi\rangle$

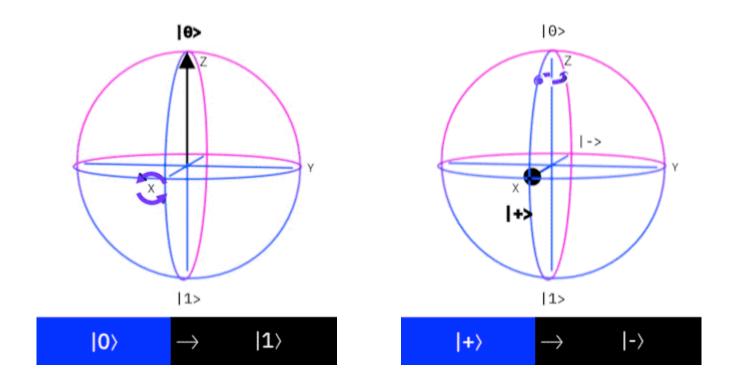
The ability to correction X-errors (bit-flips) and Z-flips (phase-flips) is sufficient to correct any coherent error.

This effect is known as the **digitisation of the error**.





Bit- and Phase-Flips



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





Logical operators and code distance

Three-qubit code:

$$|0\rangle_L = |000\rangle, \quad |1\rangle_L = |111\rangle$$

Logical X-operator *X*_{*L*} performs the mapping

$$X_L|0\rangle_L = |1\rangle_L$$
 and $X_L|1\rangle_L = |0\rangle$

For the three-qubit code:

$$X_L = X_1 X_2 X_3$$

Logical operators always commute with all the stabilisers. E.g., for the three-qubit code with stablisers Z_1Z_2 and Z_2Z_3

$$[X_1X_2X_3, Z_1Z_2] = 0$$
 and $[X_1X_2X_3, Z_2Z_3] = 0$

 \Rightarrow Logical operators always yield the `0` syndrome. I.e., they are undetectable.

The **code distance** is the equal to the minimum Hammingweight of a logical operator.

For the three-qubit code, the minimum-weight X-logical is $X_1X_2X_3$. The distance for X-errors is therefore $d_X = 3$.

However, we also have to consider Z-type logical operators.



Logical operators and code distance

Logical X-operator *X*_{*L*} performs the mapping

$$X_L|0\rangle_L = |1\rangle_L$$
 and $X_L|1\rangle_L = |0\rangle_L$

Logical Z-operator Z_L performs the mapping

 $Z_L |+\rangle_L = |-\rangle_L$ and $Z_L |-\rangle_L = |+\rangle_L$ where $|+\rangle_L = \frac{1}{\sqrt{2}}(|0\rangle_L + |1\rangle_L)$ and $|-\rangle_L = \frac{1}{\sqrt{2}}(|0\rangle_L - |1\rangle_L)$

The Z_L and X_L logical operators always anti-commute:

$$\{X_L, Z_L\} = 0$$

For the three-qubit code

$$|+\rangle_{L} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$
 and $|-\rangle_{L} = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$

A choice of logical operator for Z_L is

$$Z_L = I_1 I_2 Z_3$$
$$Z_L |+\rangle_L = \frac{1}{\sqrt{2}} (|000\rangle - |111\rangle) = |-\rangle_L$$

The Z_L operator commutes with both of the stabilisers Z_1Z_2 and Z_2Z_3 . It therefore maps to the `00` syndrome.

The **distance** of the three bit-repetition code is therefore d = 1. It can detect *X*-errors, but not *Z*-errors.



Detecting both X- and Z-Pauli errors

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

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

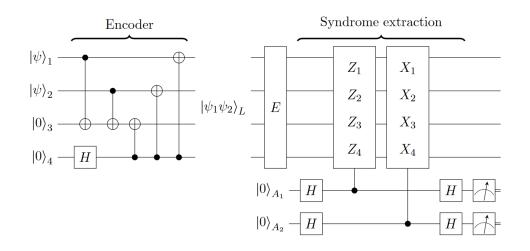
$$|01\rangle_L = \frac{1}{\sqrt{2}}(|1100\rangle + |0011\rangle)$$

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

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

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

 $X_1 X_2 X_3 X_4 Z_1 Z_2 Z_3 Z_4$



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 Distance of the [4,2,2] Code

The [[4,2,2]] detection code has **two** logical qubits. There are therefore two independent logical X-type operators: X_{L1} and X_{L2} :

$$X_{L1} = X_1 I_2 X_3 I_4$$

$$X_{L2} = X_1 X_2 I_2 I_4$$

We can obtain all of the basis states from the original $|00\rangle_L$ state using the logical operators

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

$$X_{L2}|00\rangle_L = |01\rangle_L = \frac{1}{\sqrt{2}}(|1100\rangle + |0011\rangle)$$

$$X_{L1}|00\rangle_L = |10\rangle_L = \frac{1}{\sqrt{2}}(|1010\rangle + |0101\rangle)$$

$$X_{L1}X_{L2}|00\rangle_L = |11\rangle_L = \frac{1}{\sqrt{2}}(|0110\rangle + |1001\rangle)$$

To find the Z-logical operators, we need to find operators Z_{L1} and Z_{L2} that:

- 1. Commute with all the stabilisers
- 2. Anti-commute with X_{L1} and X_{L2}

Two logical operators that satisfy these conditions are:

$$Z_{L1} = Z_1 Z_2 I_3 I_4 Z_{L2} = Z_1 I_2 Z_3 I_4$$

Distance of the [4,2,2] code

- The logical operators are: $X_1I_2X_3I_4$, $X_1X_2I_2I_4$, $Z_1Z_2I_3I_4$, $Z_1I_2Z_3I_4$
- There are no-single qubit errors that yield the `00` syndrome when the stabilisers are measured.
- Therefore, the minimum-weight undetectable error has weight 2
- The distance of the code is d = 2. It is a valid detection code for both Pauli-X and Pauli-Z type errors.



The [[n,k,d]] notation

Quantum codes are usually labelled using the [[n, k, d]] notation. This represents the following parameters.

- *n*: the number of physical qubits
- *k*: the number of logical qubits
- *d*: the code distance

Detection codes vs. correction codes

Detection codes have d = 2

Correction codes (next lecture) have $d \ge 3$.

Example 1: the detection code on the previous slide has parameters [[n=4,k=2,d=2]].

Example 2: the three-bit repetition code has parameters [[3,1,1]].





THE UNIVERSITY of EDINBURGH informatics

www.informatics.ed.ac.uk