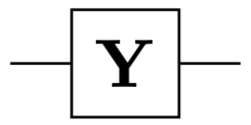
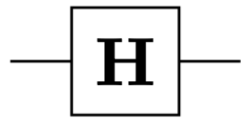
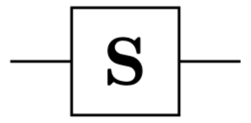
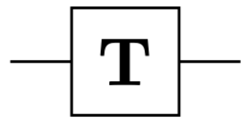
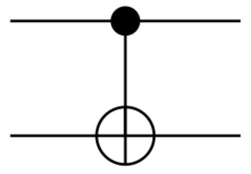
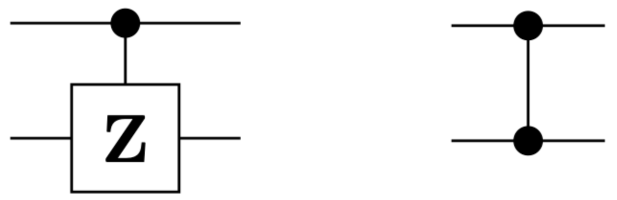
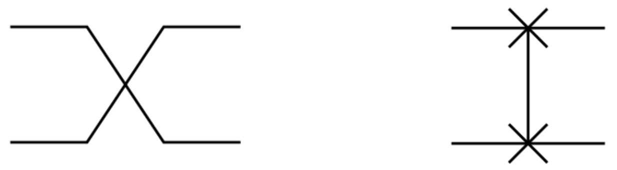
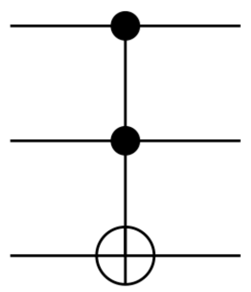
Quantum Error-Correction

without it quantum computing would not be possible

CANDIDATE: ALEXANDER FERRARO

SUPERVISOR: PHILIPP HAUKE

Operator	Gate(s)	Matrix
Pauli-X (X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Quantum computation and necessity of quantum error correction

- Quantum computers are based on qubits as unit of information:

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

- Qubits properties of quantum mechanics: such as quantum entanglement and superposition

- One can operate on qubits through logic gates.

- Qubits are delicate objects and it is impossible to isolate completely.

- Noise can act on quits

FERRARO ALEXANDER, 21/09/2021

Quantum errors

The most general approach is to describe the error with CPTP maps:

$$\rho \to \sum_k E_k \rho E_k^\dagger \quad with \quad \sum_k E_k^\dagger E_k = 1.$$

Example of single qubit error:

X error or Bit Flip:

$$\alpha|0\rangle + \beta|1\rangle \to X|\psi\rangle \to \alpha|1\rangle + \beta|0\rangle$$

Z error Phase flip:

$$\alpha|0\rangle + \beta|1\rangle \to Z|\psi\rangle \to \alpha|0\rangle - \beta|1\rangle$$

General rotation:

$$R_\phi|\psi\rangle \to cos(\frac{\phi}{2})I|\psi\rangle - \mathbf{i}sin(\frac{\phi}{2})Z|\psi\rangle$$

Inspiration from the classic

- Repetition code:

  $0 \rightarrow 000$

  $1 \rightarrow 111$

- Then suppose a bit-flip error happens:

  $000 \ \rightarrow error \rightarrow 100$

- We can restore the initial bit by majority vote:

  $100 \ \rightarrow correction \rightarrow 000$

quantum problems

- We cannot copy an arbitrary state: No-cloning theorem

$$|\psi\rangle \not\rightarrow |\psi\rangle|\psi\rangle|\psi\rangle$$

- Looking at the state destroys the information the superposition

- Correct multiple errors not only bit flip.

- Continuous errors (continuous phase rotation)

3 Bit-Flip Code

- We cannot clone–> spread the information (Encoding procedure).

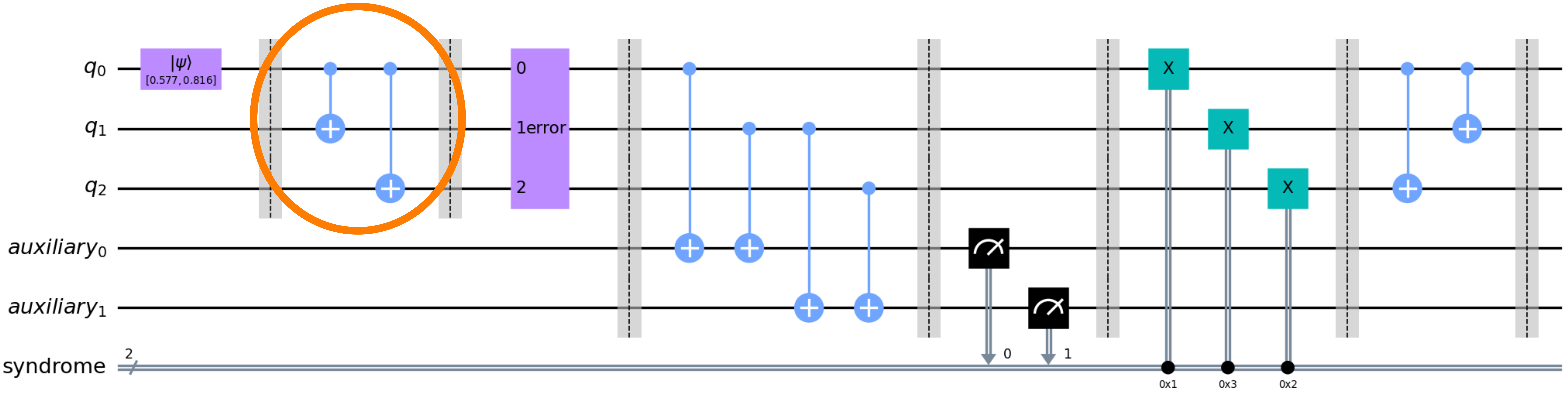
  From: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle \rightarrow \alpha|0\rangle_L + \beta|1\rangle_L$

  We don't copy we use entangled state to spread the information and protect it.

- The space spanned by $\{|000\rangle, |111\rangle\}$ is called code space and its elements are the codewords.

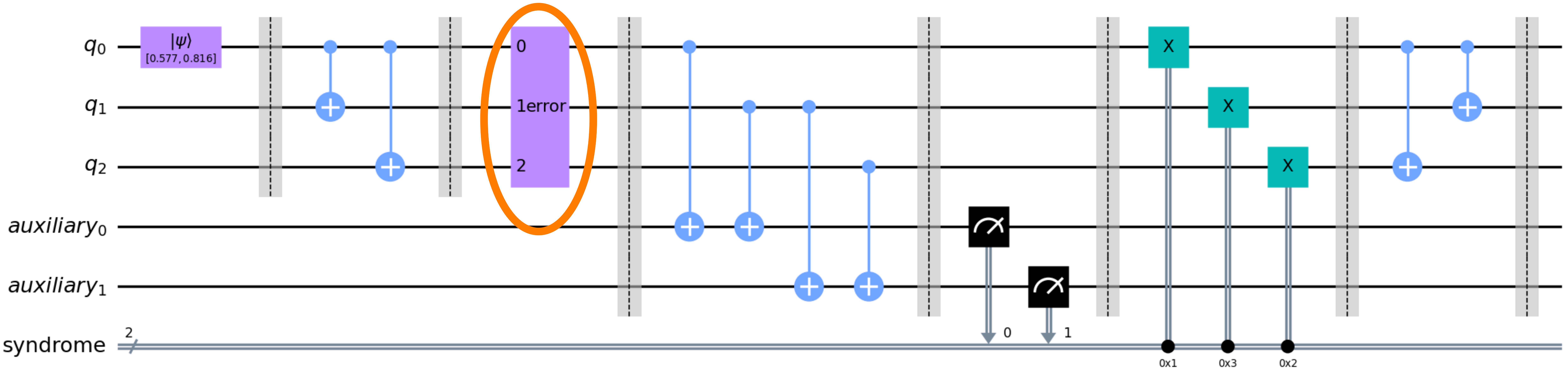
In this simulation the data qubit is prepared in:

$$|\psi\rangle = \frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$$

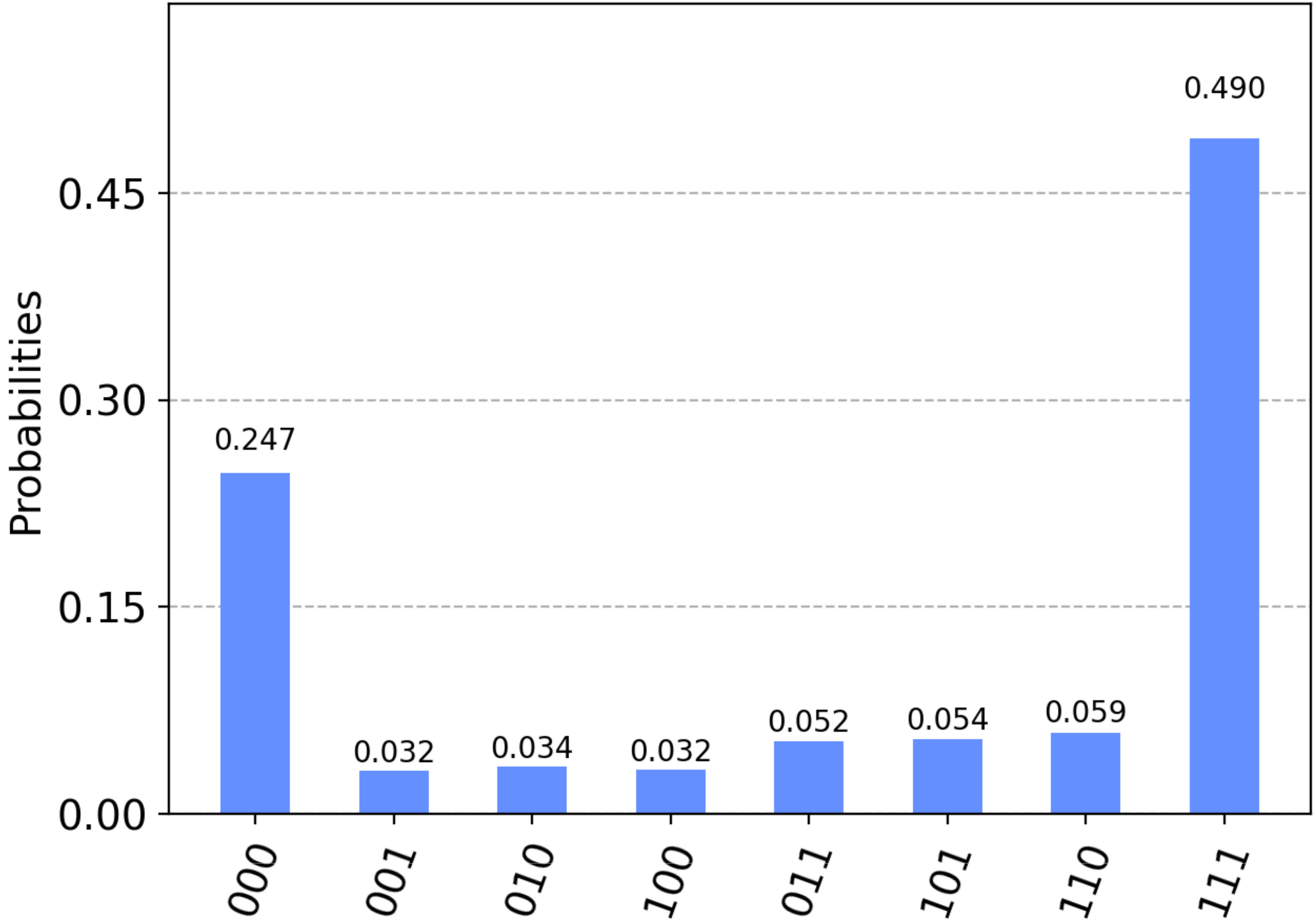


3 Bit-Flip Code: noise assumption

- The noise applies X with probability p and I with probability (1-p)
- it acts independently and it is identically distributed on each qubit
- only the channel is an error source
- probability for the 3 qubit code has to be less that $p < \dfrac{1}{2}$

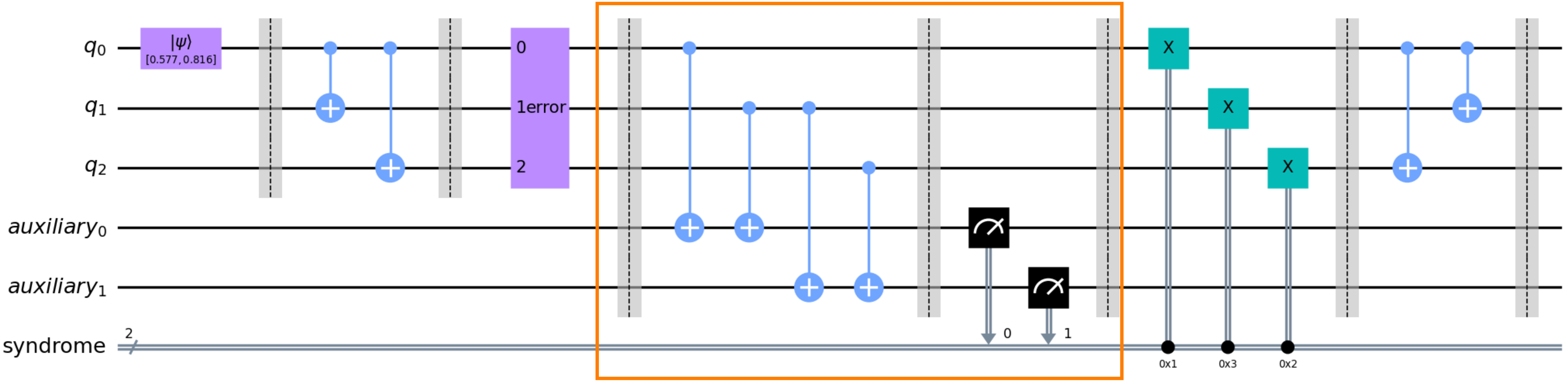


Measurement just after the error



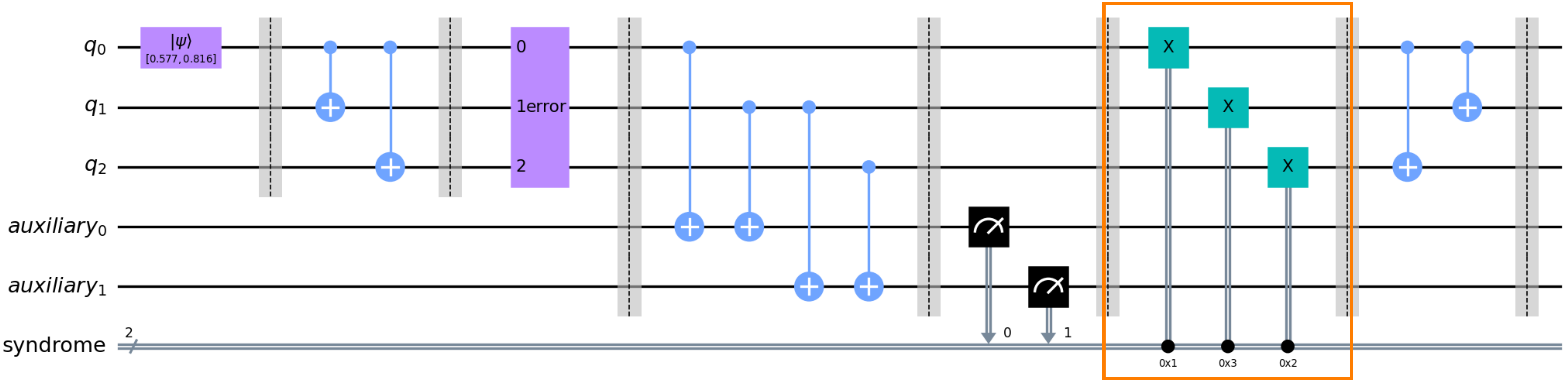
3 Bit-Flip Code

- Suppose a bit flip error happens on the second qubit: $\alpha|000\rangle + \beta|111\rangle \rightarrow X_2 \quad error \rightarrow \alpha|010\rangle + \beta|101\rangle$
- Syndrome measurement: Detect which error occurred without getting information from the state.
- **<u>We measure the error not the state!</u>**
- One way to do this is to measure the fact that one qubit is different from the other two. In practice we store the results in the ancillas.

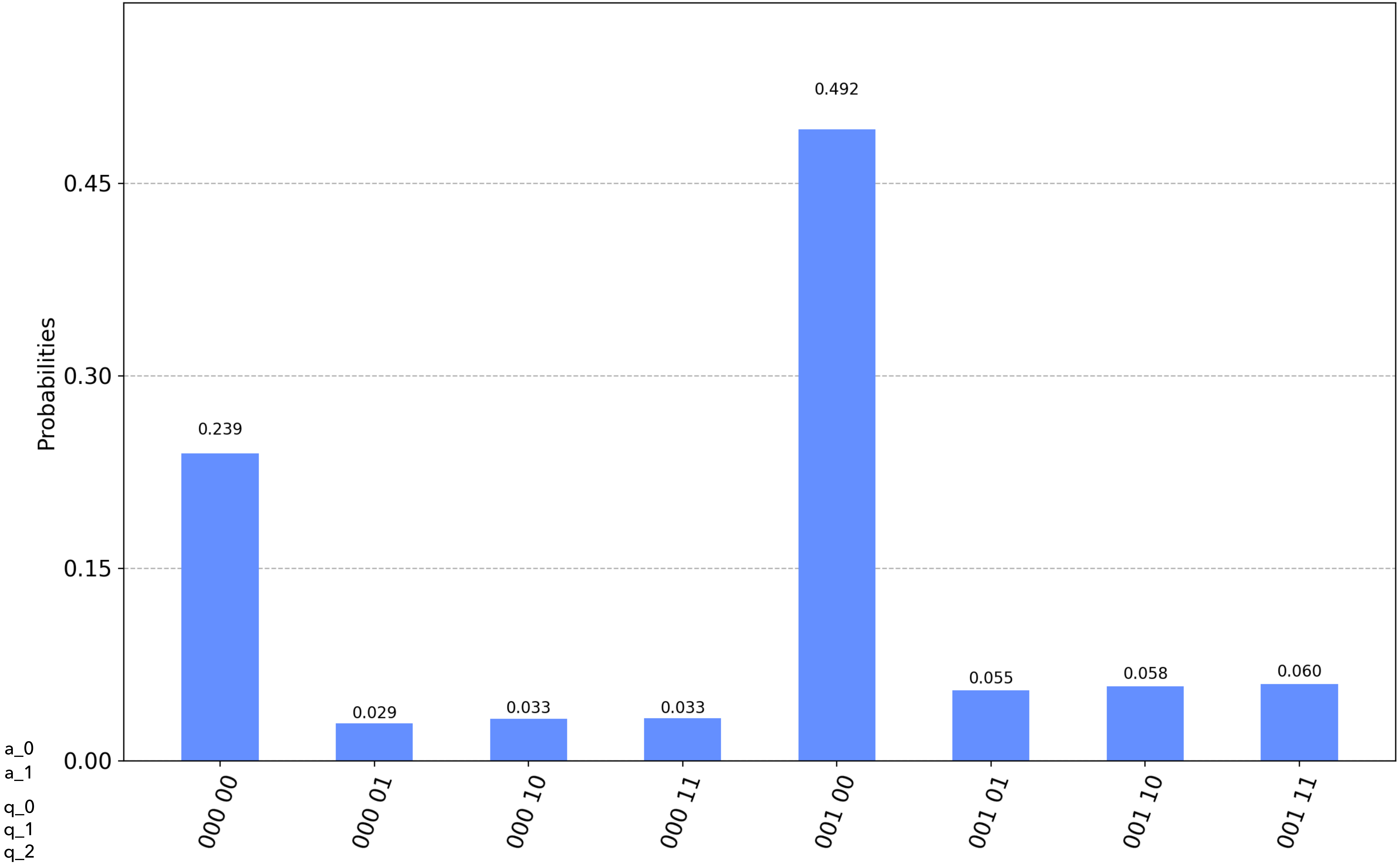


3 Bit-Flip Code: Syndrome measurement

Syndrome measurement: $(Z_1 Z_2, Z_2 Z_3)$	Ancilla state	Correction
$(+1, +1)$	$\|00\rangle$	Clean state, no correction needed
$(-1, +1)$	$\|10\rangle$	Bit flip on qubit 1
$(-1, -1)$	$\|11\rangle$	Bit flip on qubit 2
$(+1, -1)$	$\|01\rangle$	Bit flip on qubit 3

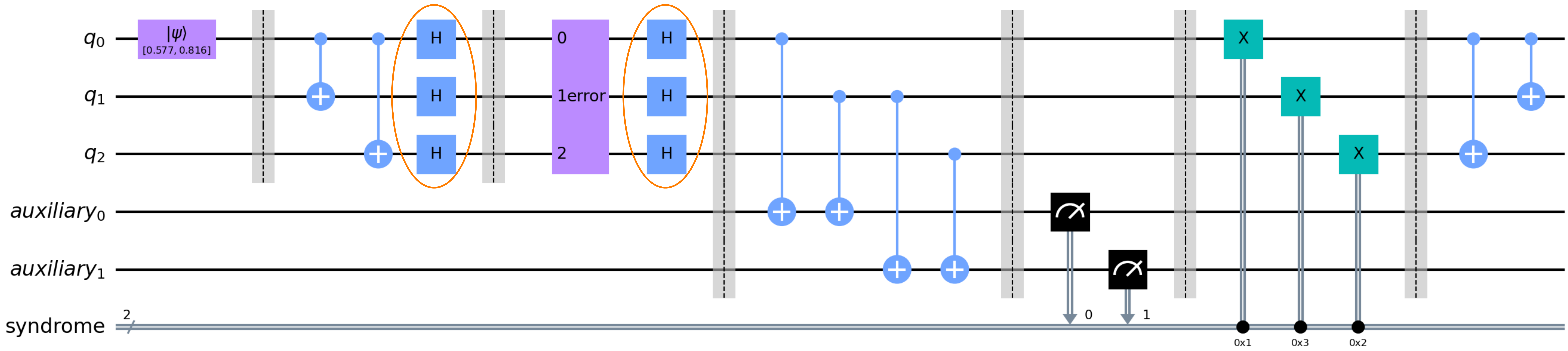


Measurement after error correction



Phase flip code

- A phase shift can be viewed as a bit flip in the computational basis:
- $$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$
- In fact: **HZH=X**



Fidelity

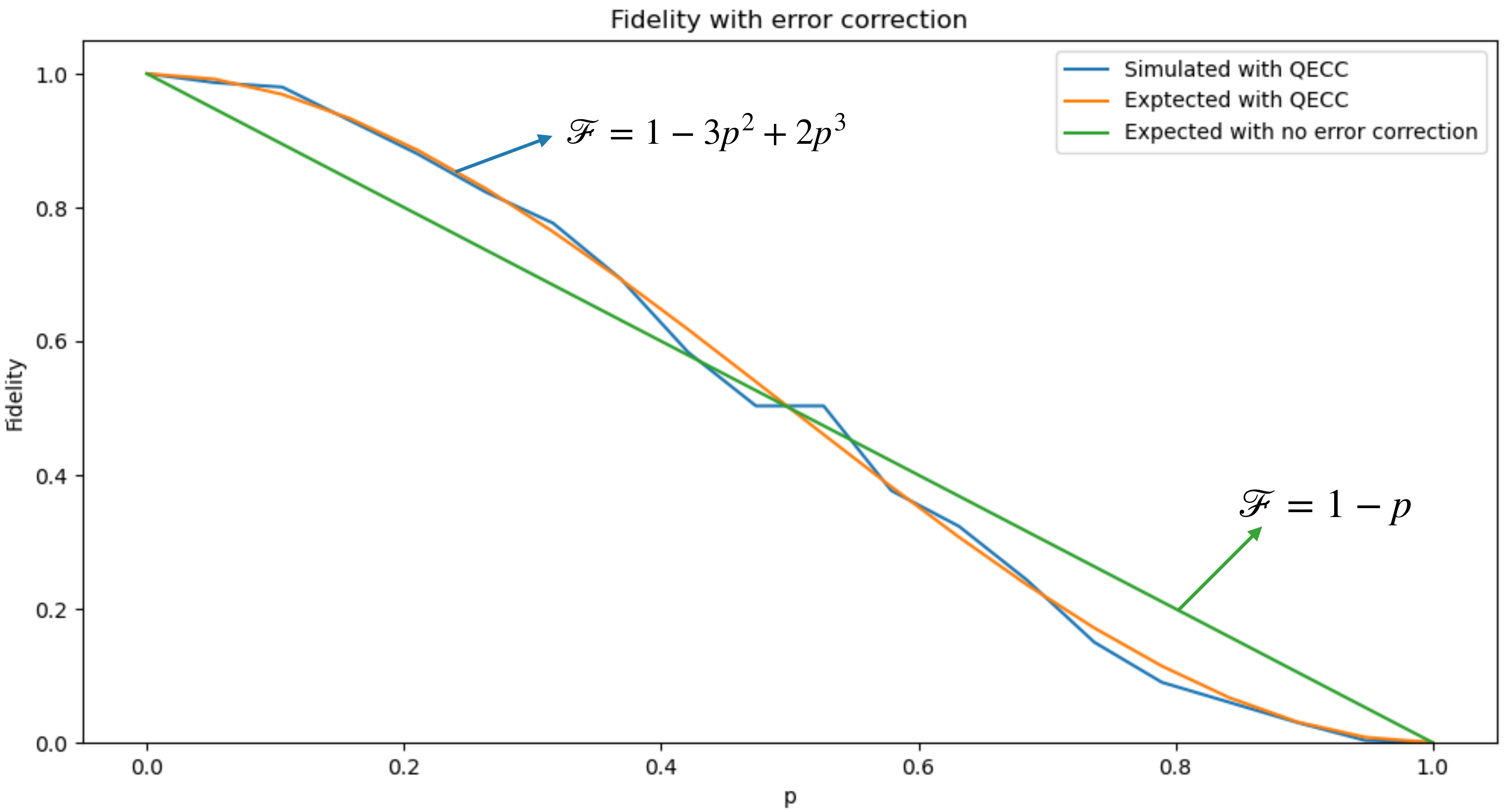
The fidelity is a quantity that can represent the similarity between the initial and final state, it can give an appropriate measurement of the quality of the code:

$$\mathcal{F}(\rho, |\psi_i\rangle) = \langle\psi_i|\rho|\psi_i\rangle$$

We don't know the state in advance, we need to use the minimum fidelity:

$$\mathcal{F}(\rho, |\psi\rangle) = min_\psi\langle\psi|\rho|\psi\rangle$$

Is the 3 qubit code worth the efforts?


Fidelity with error correction
Simulated with QECC
Exptected with QECC
Expected with no error correction
$\mathcal{F} = 1 - 3p^2 + 2p^3$
$\mathcal{F} = 1 - p$
Fidelity
p
1.0
0.8
0.6
0.4
0.2
0.0
0.0
0.2
0.4
0.6
0.8
1.0

Stabiliser formalism

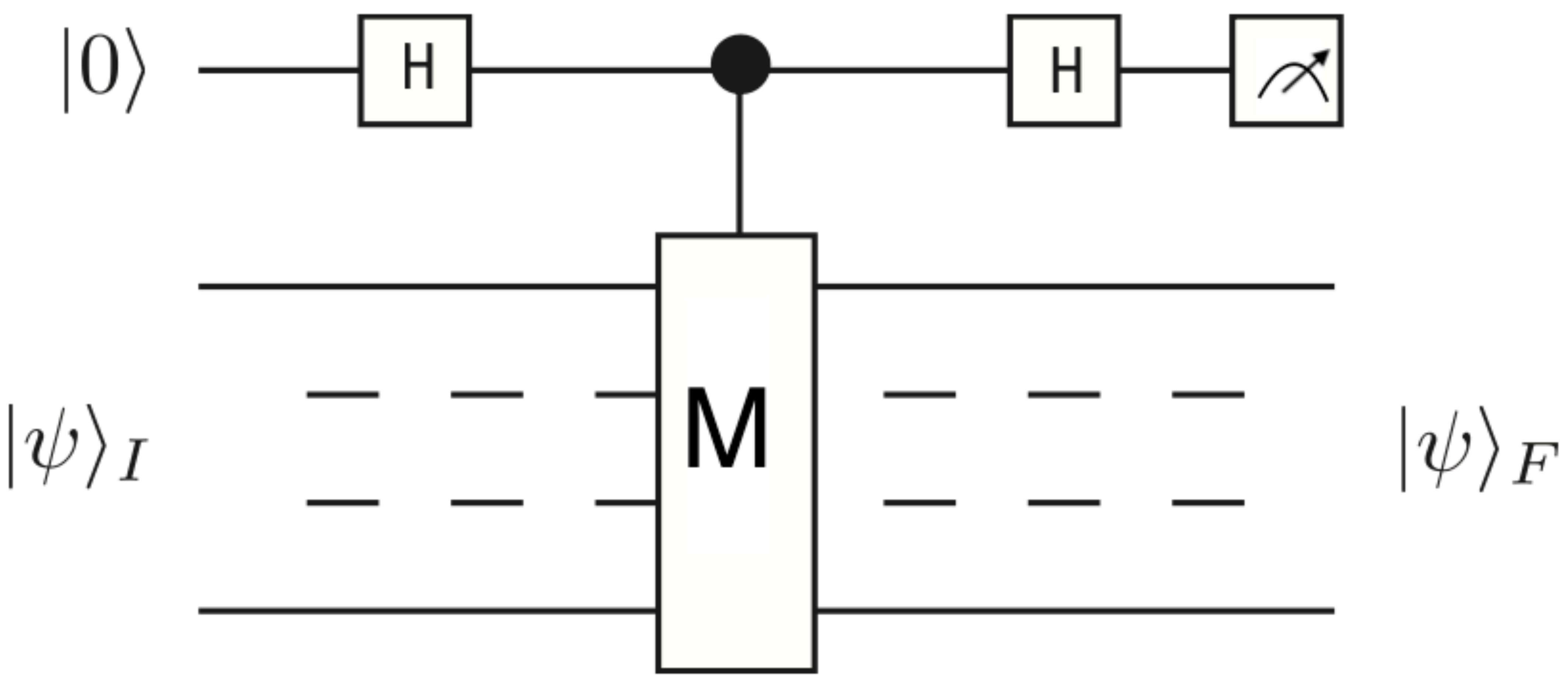
- Phase and bit flip act on the same circuit,
- Numbers of qubits start rising is difficult to take into account all the possible scenarios.
- We can rephrase the syndromes using the stabiliser formalism, via measurement of commuting operator.
- Elements of stabiliser set $\mathscr{S}$ must satisfy this:

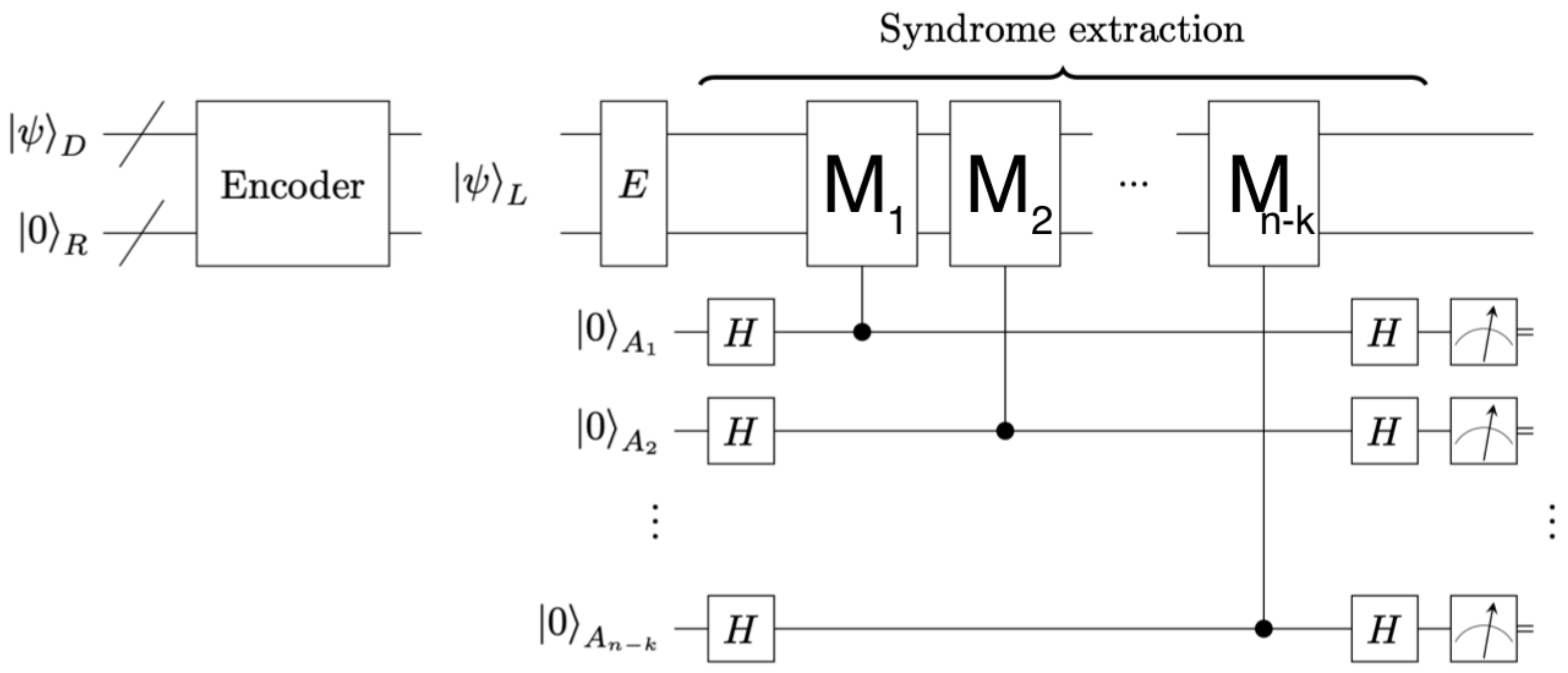
$$M|u\rangle = |u\rangle \quad \forall u \in \mathscr{C}, \quad \forall M \in \mathscr{S} \, .$$

- Codewords are eigenstate of stabilisers.
- Suitable set of stabiliser is the Pauli group.
- An error E can commute or anticommute with the stabilisers:

$$M(E|\psi\rangle_L) = \pm EM|\psi\rangle_L = \pm (E|\psi\rangle_L)$$

- If we look to the eigenvalue of the generators of the stabiliser set, we can get information about the error.





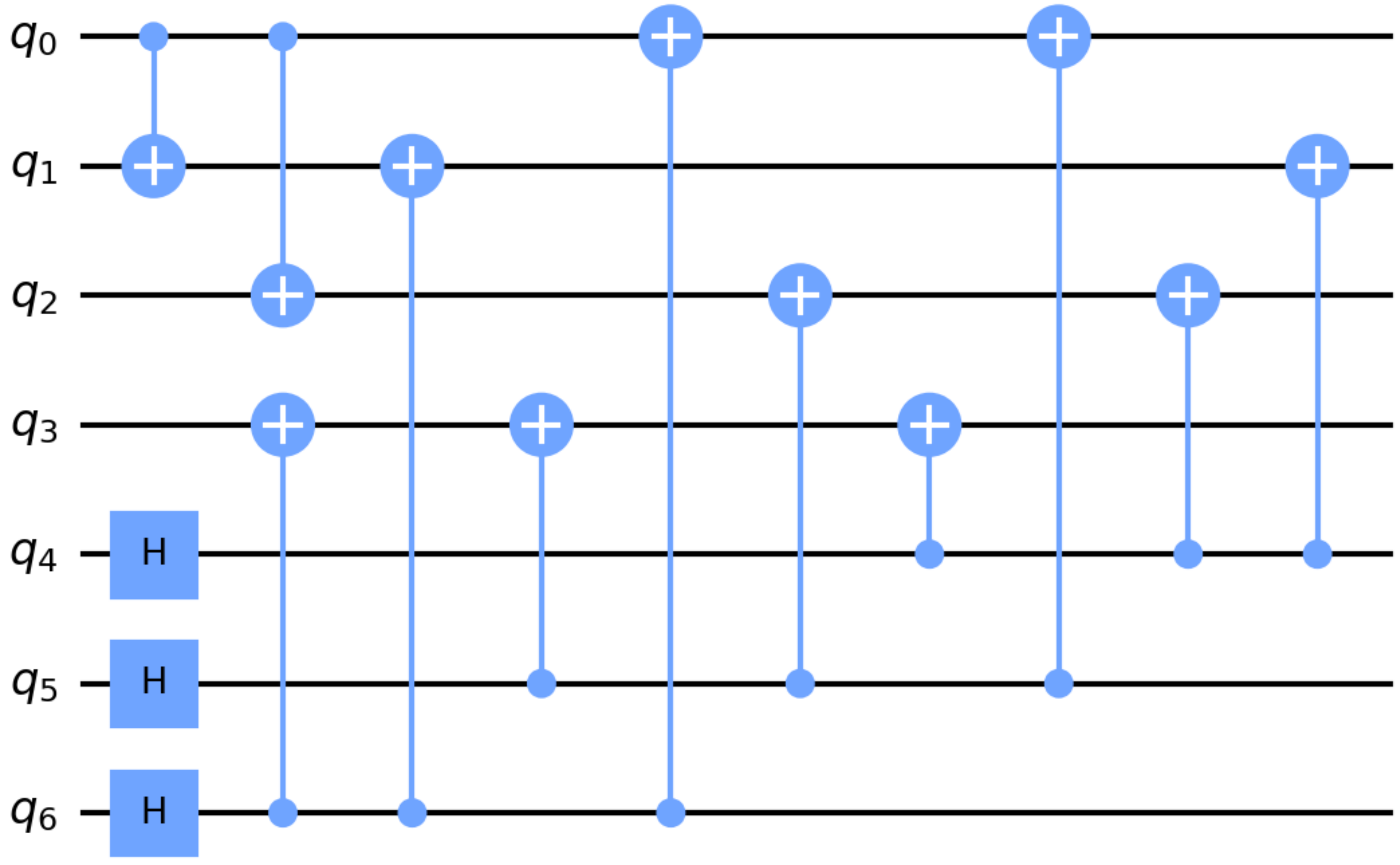
Syndromes with Stabilisers

- Only n-k stabiliser are needed
- We can operate directly on encoded states
- $|\psi\rangle_{System} = \frac{1}{2}\left(|\psi\rangle_I + \lambda|\psi\rangle_I\right)|0\rangle + \frac{1}{2}\left(|\psi\rangle_I - \lambda|\psi\rangle_I\right)|1\rangle$
- So if we measure $|1\rangle$ from the ancilla we know that an error has occured
- Repeating the process for all the n-k stabilisers gives us a string associated with the error:

$$|0\rangle_a \sum_i \left(E_i|\psi\rangle_L\right) \rightarrow \sum_i \left|s_i\right\rangle_a \left(E_i|\psi\rangle_L\right).$$

CSS codes

- Sometimes is difficult to find a stabiliser set from the very beginning. We can recycle from classical codes.



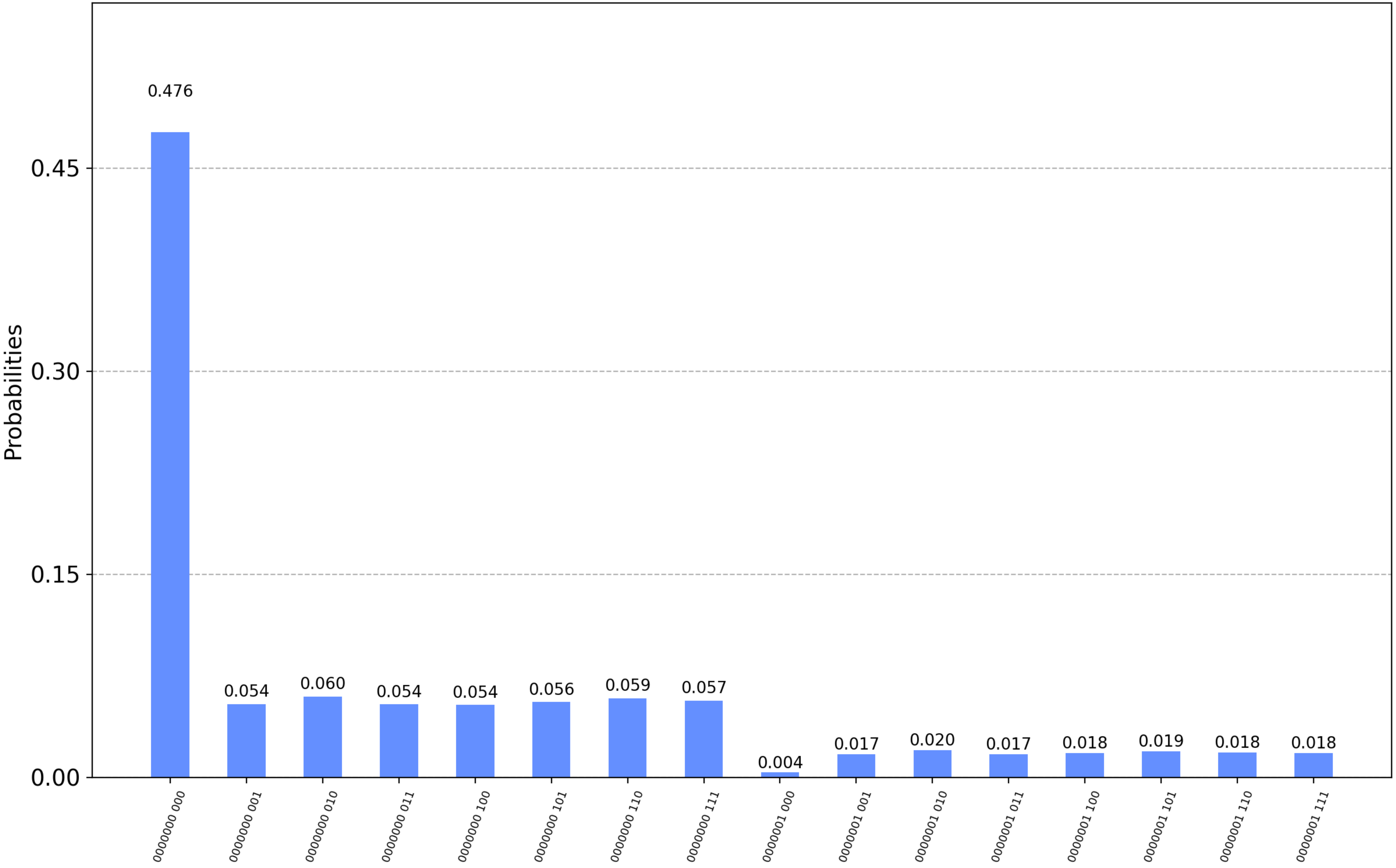
$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

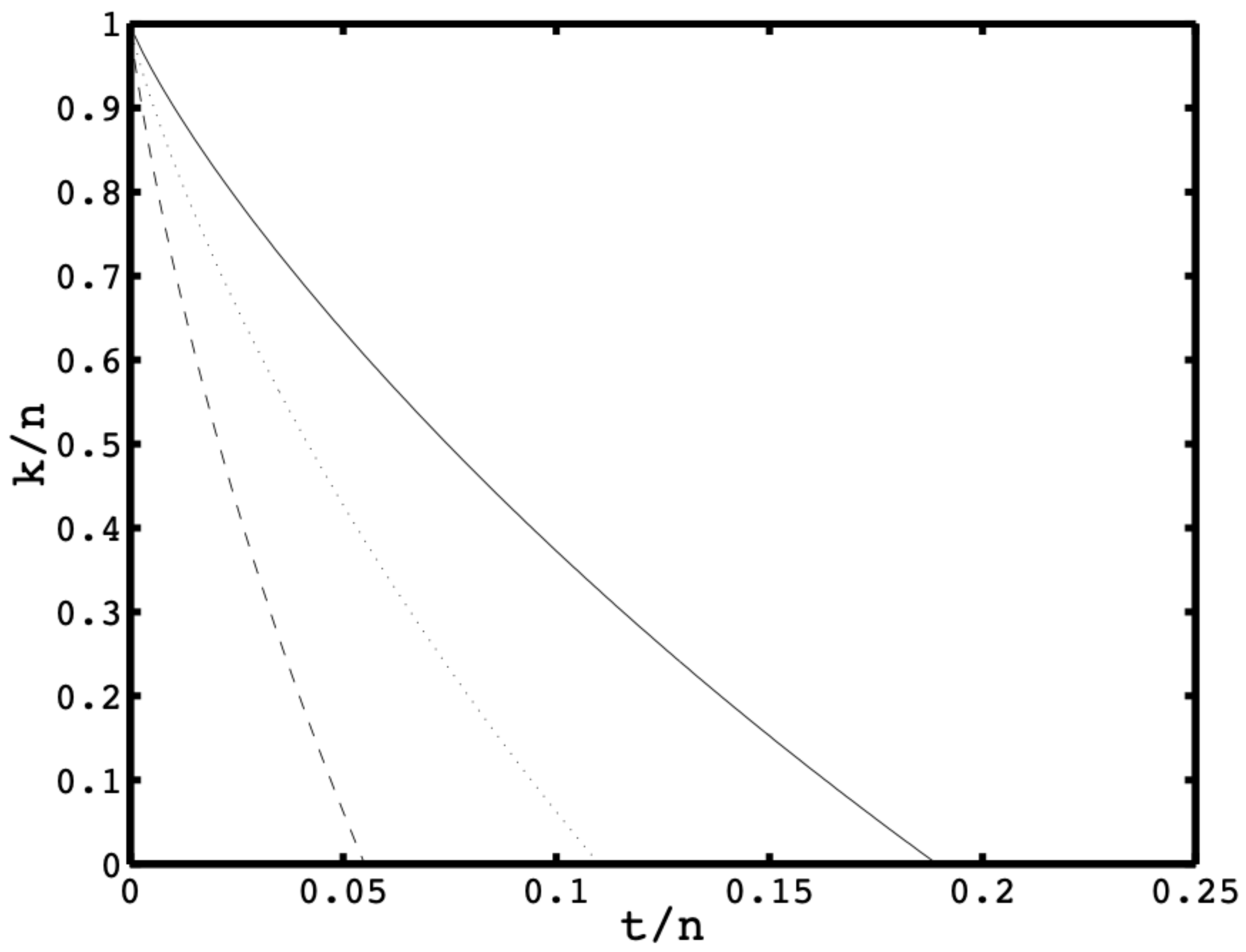
$$|0\rangle_L = \frac{1}{\sqrt{8}}[|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle]$$

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

$$\mathcal{S}: \begin{matrix} I & I & I & Z & Z & Z & Z \\ I & Z & Z & I & I & Z & Z \\ Z & I & Z & I & Z & I & Z \\ I & I & I & X & X & X & X \\ I & X & X & I & I & X & X \\ X & I & X & I & X & I & X \end{matrix}$$

Steane 7 qubit code simulation, only X errors





$$\left(\sum_{j=0}^{t} 3^j \binom{n}{j} \right) 2^k \leq 2^n .$$

Hamming bound

- Can we do better?
- Yes, the best that we can create for a single code is to encode 1 qubit in 5 physical one, and the code can correct up to 1 error.

- Quantum Hamming bound:

  $j \rightarrow$ all the possible weight of error

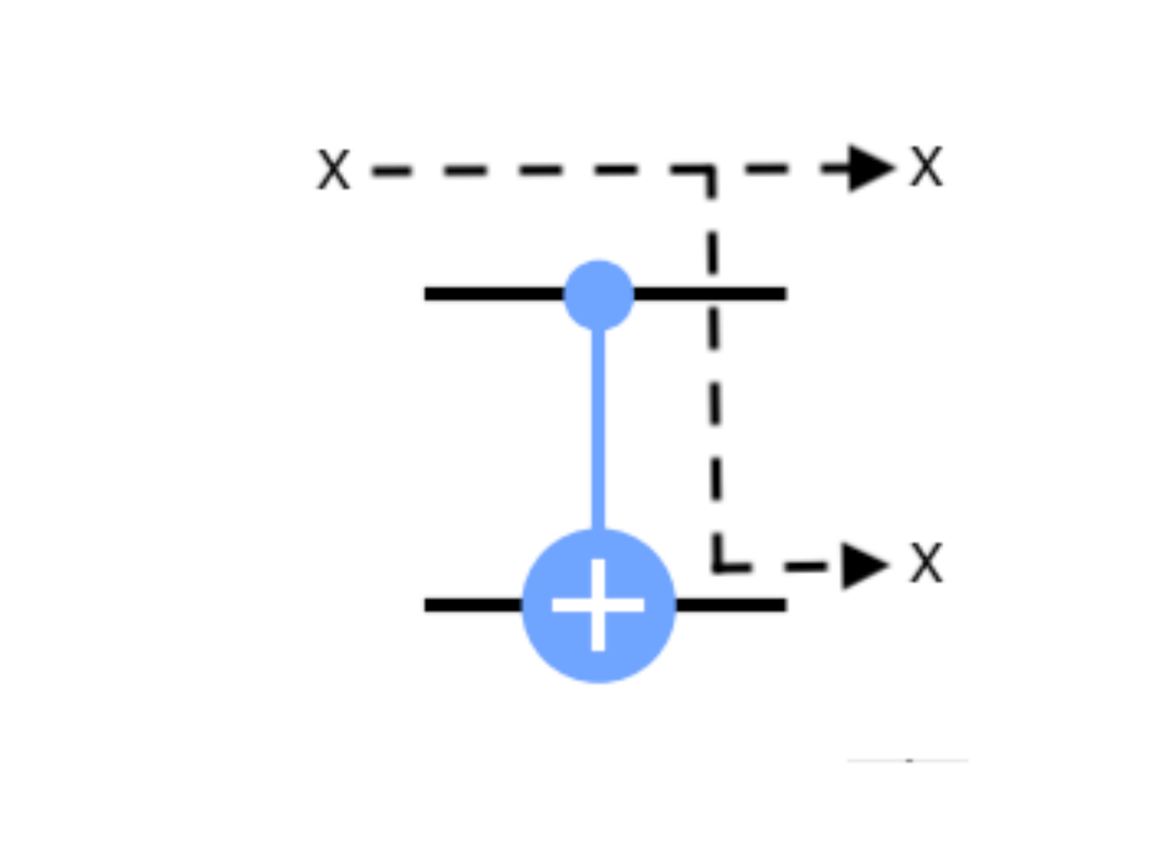
  $\binom{n}{j} \rightarrow$ location of error

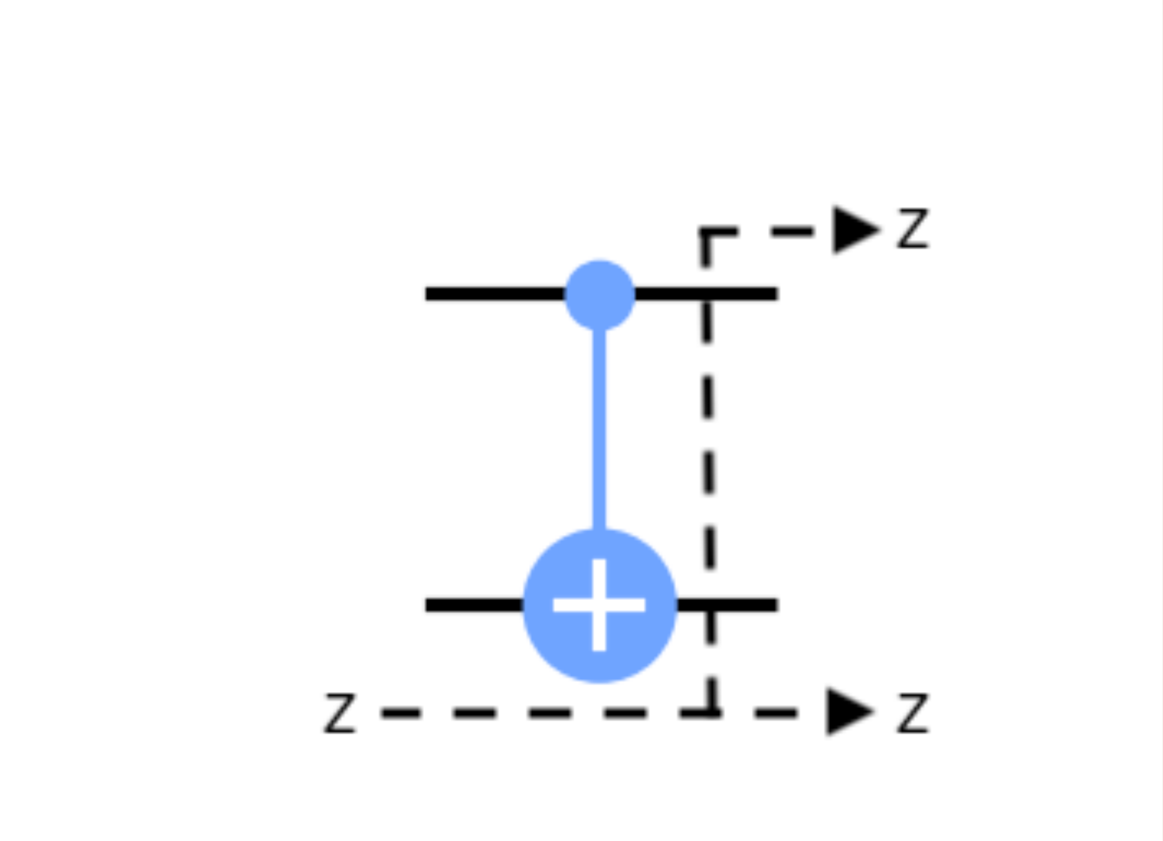
  $3^j \rightarrow$ 3 possible error (X,Y, Z)

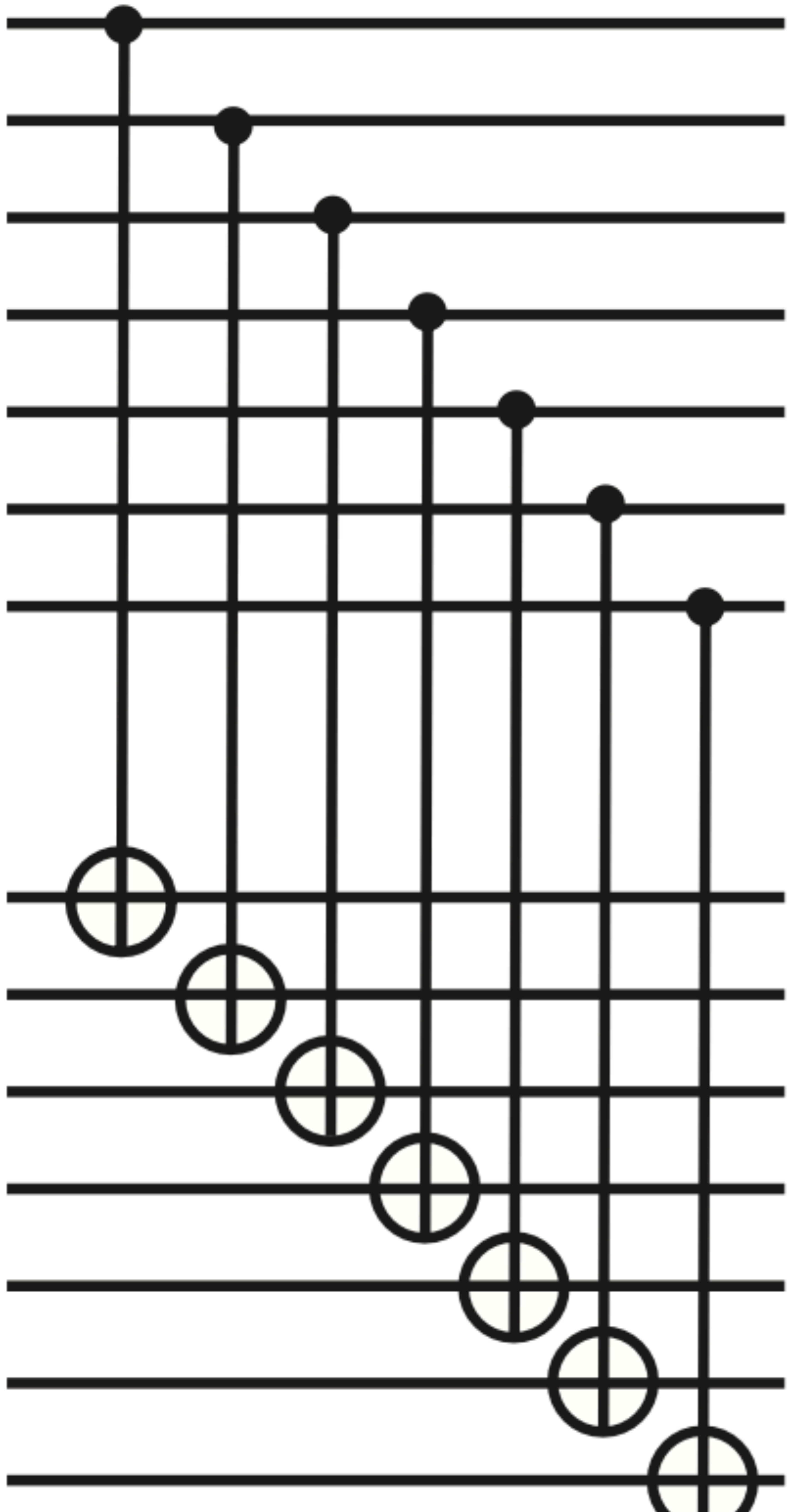
  $2^k \rightarrow$ dimension logical space
  $2^n \rightarrow$ total space

Fault tolerant computation and error propagation

- computes directly on encoded quantum







Fault tolerant gates

- Implement in transversal way, through encoded blocks. In this way we shift the probability to not be able to correct the error from $p \to cp^2 \quad where \quad c < \frac{1}{p}$, we want the prob to decrease.
- Only with CNOT, Hadamard, Rotation $\pi/4$ gate we cannot reach universal computation $UE|\psi\rangle = \left(UEU^\dagger\right) U|\psi\rangle$
- Need a gate more : Toffoli or $\pi/8$ rotation gate
- $\pi/8$ rotation gate implemented in a fault-tolerant way through teleportation protocols

Threshold theorem

- It says that if the error rate of a physical system is below some threshold value, arbitrarily long reliable fault-tolerant quantum computation is possible
- 2 procedure: Concatenation and fault-tolerant gates

$$
\begin{array}{ccccccccc}
\text{level } 0 & & \text{level } 1 & & \text{level } 2 & & \dots & & \text{level } k \\
p & \to & cp^2 & \to & c^{-1}\left(cp^2\right)^2 & \to & \dots & \to & c^{-1}(cp)^{2^k}
\end{array}
$$

$$
\begin{array}{ccccccccc}
\text{level } 0 & & \text{level } 1 & & \text{level } 2 & & \dots & & \text{level } k \\
T & \to & NT & \to & N^2T & \to & \dots & \to & N^kT
\end{array}
$$

Threshold theorem

- Achieve total error rate is below a certain ε: $Tp_k < \varepsilon$,
  T are the number of logical gates to implement.
- we can achieve fault tolerant computation with only :
  #gates $\sim O(T\,\mathrm{poly}(\log T/\epsilon))$.

Conclusions