A primer of Quantum Error Correction codes

Rajni Bala and Sooryansh Asthana

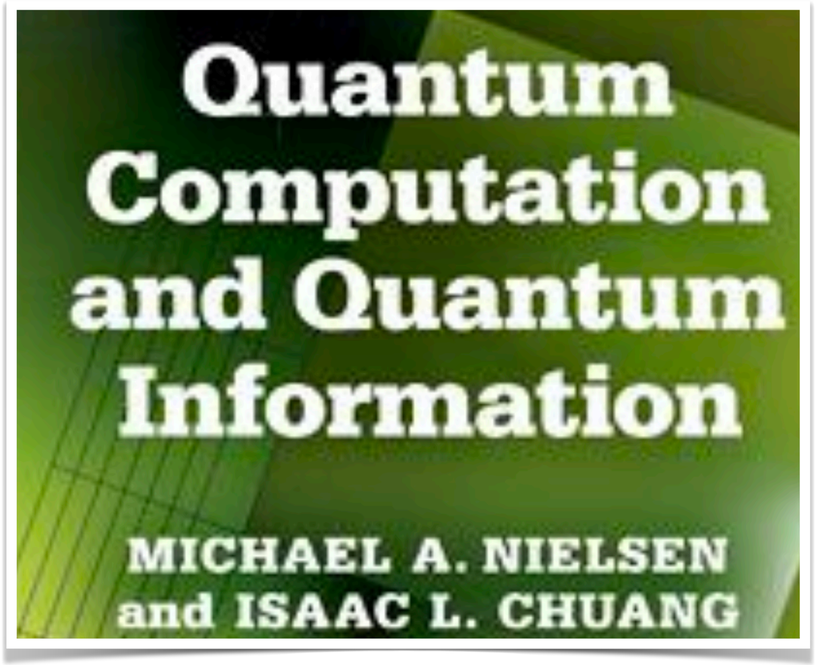
Supervisor: Prof. V. Ravishankar

Department of Physics, IIT Delhi

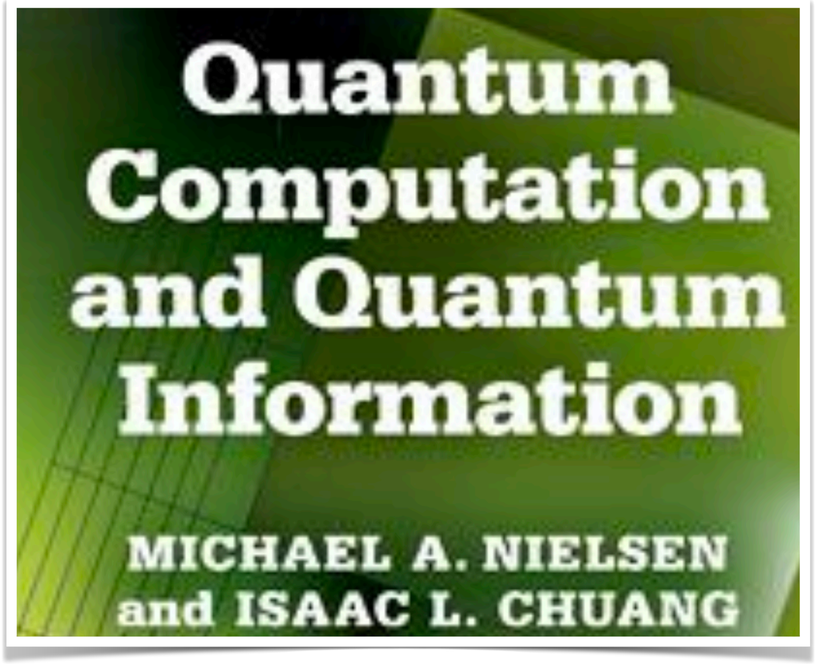
rajnisharma813@gmail.com
sooryanshasthana@gmail.com

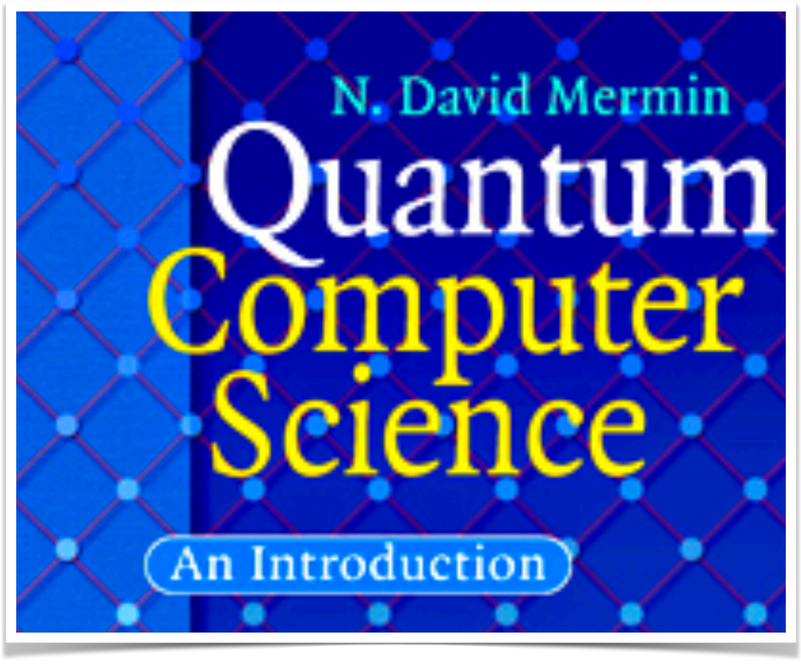
One Week High-End Workshop
On
Quantum computing and information
(22nd-28th July)

References

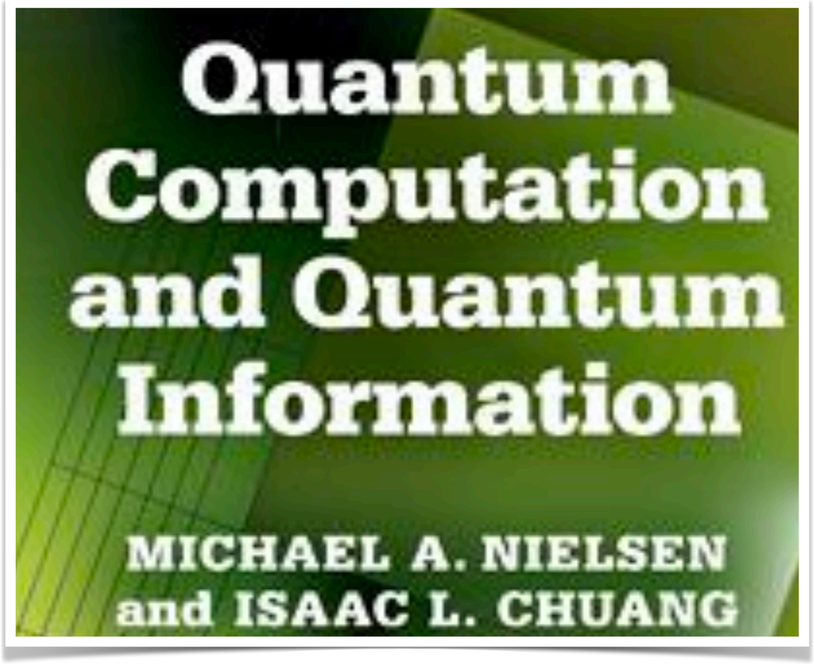

Quantum
Computation
and Quantum
Information
MICHAEL A. NIELSEN
and ISAAC L. CHUANG

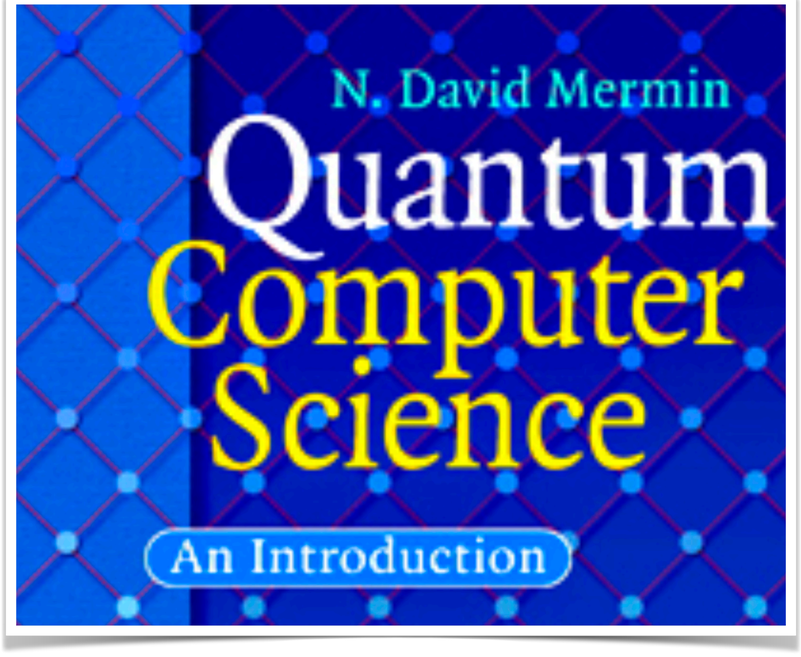
References

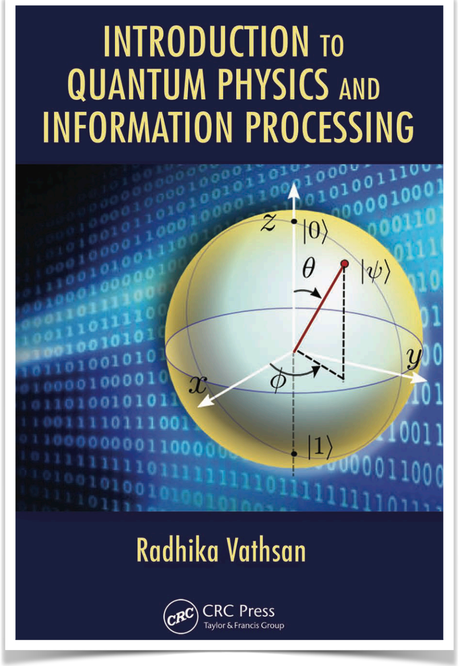

Quantum Computation and Quantum Information
MICHAEL A. NIELSEN and ISAAC L. CHUANG


N. David Mermin
Quantum Computer Science
An Introduction

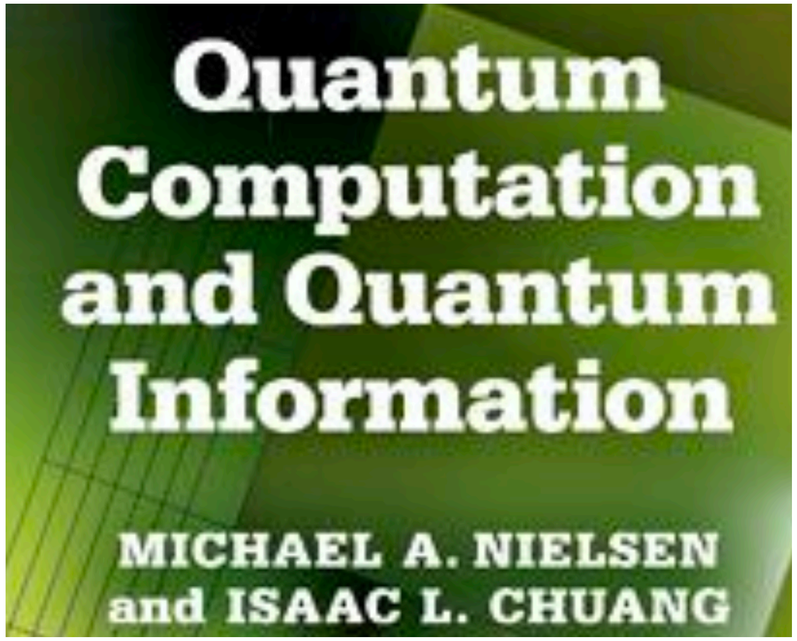
References

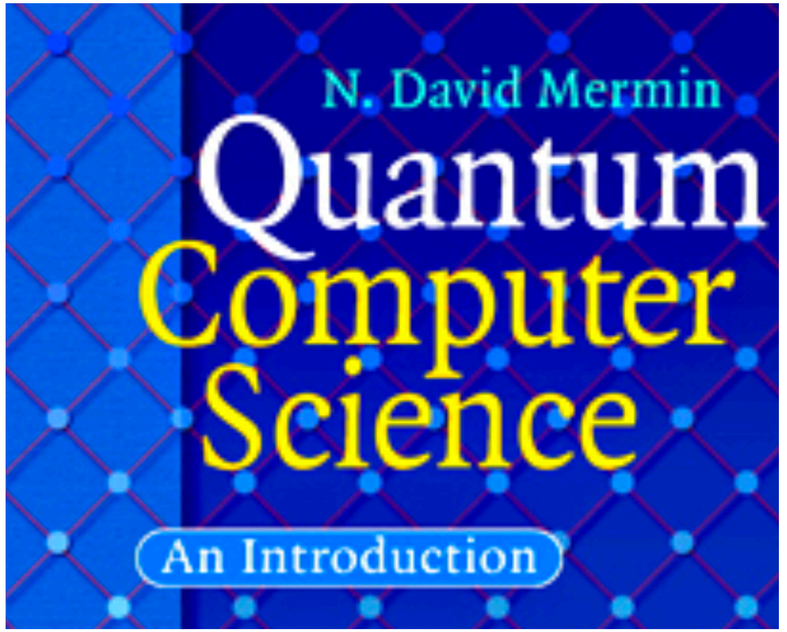

Quantum Computation and Quantum Information
MICHAEL A. NIELSEN and ISAAC L. CHUANG

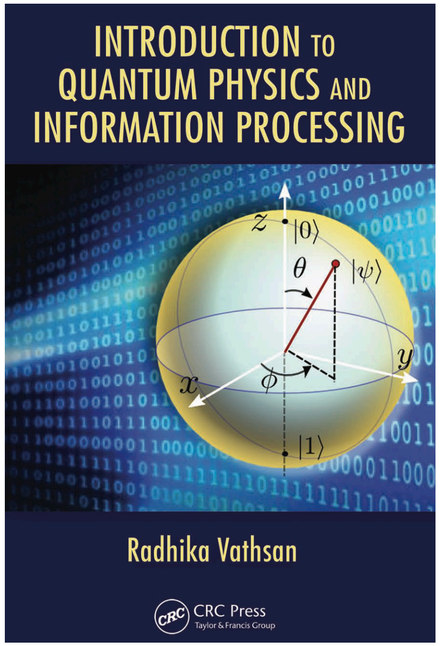

N. David Mermin
Quantum Computer Science
An Introduction


INTRODUCTION TO QUANTUM PHYSICS AND INFORMATION PROCESSING
Radhika Vathsan
CRC Press
Taylor & Francis Group

References







Google

Outline

- Need for Quantum error correction
- Basic ideas underlying quantum error correction
- Quantum entanglement as a resource in error correction

Quantum computing and communication: elegant protocols

- Deutsch-Jozsa algorithm: identify between two different kinds of functions
- Simon’s algorithm: period-finding algorithm
- Shor’s algorithm: prime factorisation

Quantum computing and communication: elegant protocols

- Deutsch-Jozsa algorithm: identify between two different kinds of functions
- Simon's algorithm: period-finding algorithm
- Shor's algorithm: prime factorisation

- Quantum teleportation: teleporting a quantum state
- Superdense coding: sending two bits of info with one qubit transfer
- Quantum key distribution: secure communication

General idea

Use

(i) quantum bits (qubits),

(ii) quantum operations,

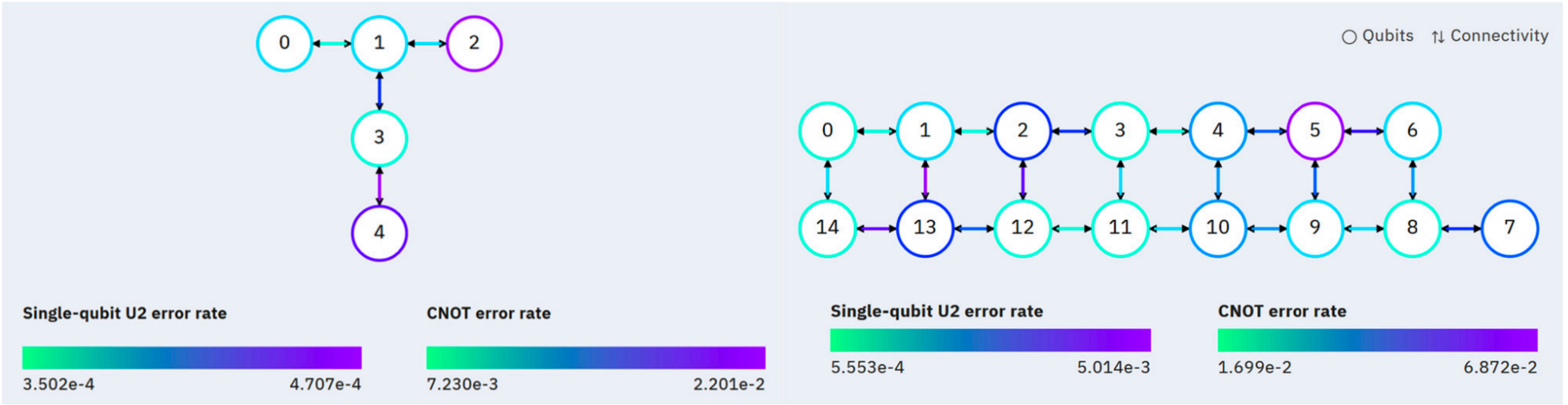
(iii) quantum features

to perform tasks.

New technology, new challenges

New technology, new challenges

Error rates on IBM



(a) (b)

Understanding and compensating for noise on IBM quantum computers

Scott Johnstun and Jean-François Van Huele

American Journal of Physics **89**, 935 (2021)

Errors in different circuits

One qubit circuit				
Outcome	$\|0\rangle$	$\|1\rangle$		
Simulation	0.482	0.518		
Experiment	0.538	0.462		
Entangling circuit				
Outcome	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
Simulation	0.495	0	0	0.505
Experiment	0.458	0.047	0.061	0.434
Phase estimator circuit				
Outcome	$\|000\rangle$	$\|001\rangle$	$\|010\rangle$	$\|011\rangle$
Simulation	0.405	0.088	0.077	0.430
Experiment	0.484	0.149	0.033	0.085
Outcome	$\|100\rangle$	$\|101\rangle$	$\|110\rangle$	$\|111\rangle$
Simulation	0	0	0	0
Experiment	0.152	0.055	0.024	0.018

Understanding and compensating for noise on IBM quantum computers

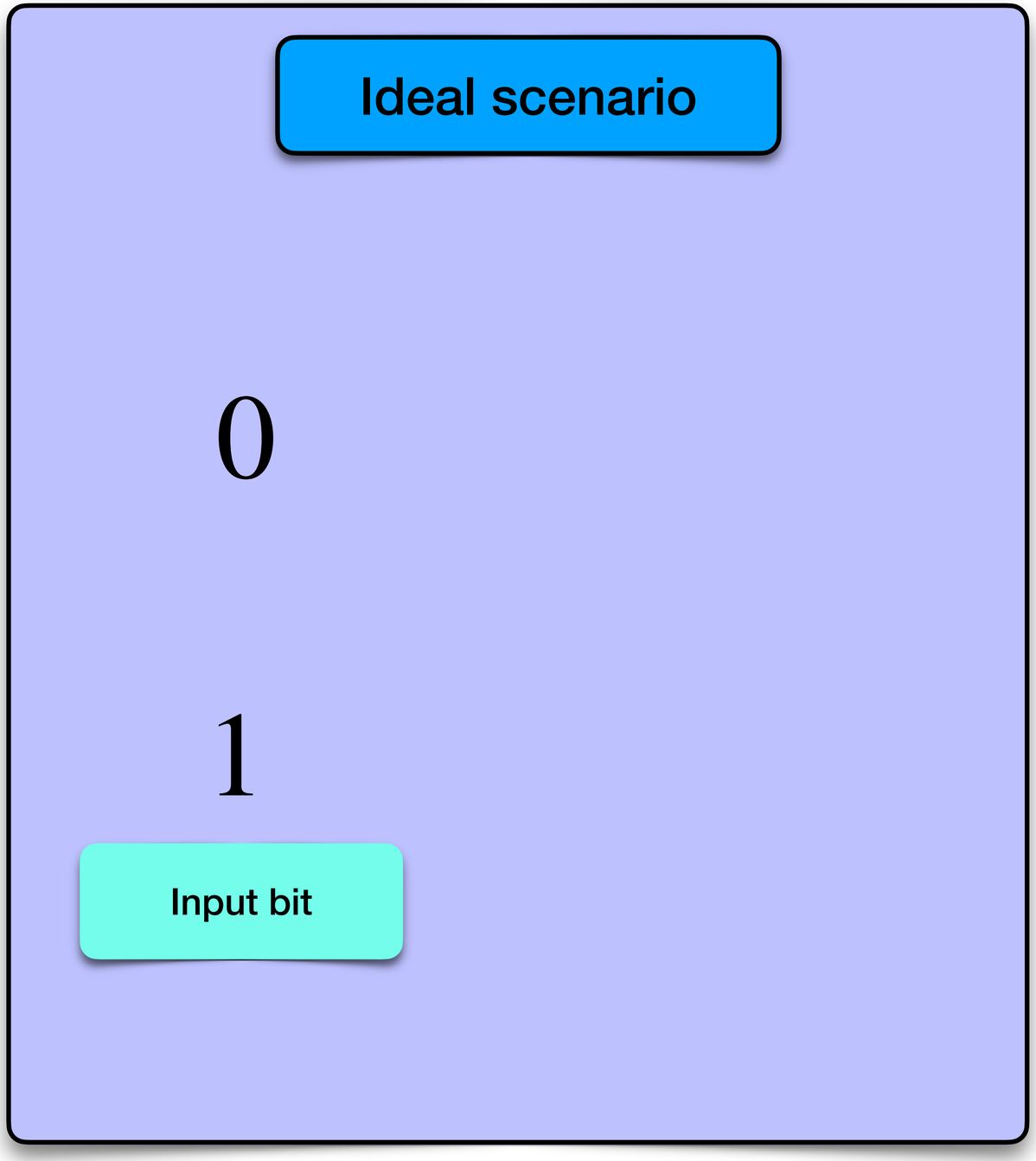
Scott Johnstun and Jean-François Van Huele
American Journal of Physics **89**, 935 (2021)

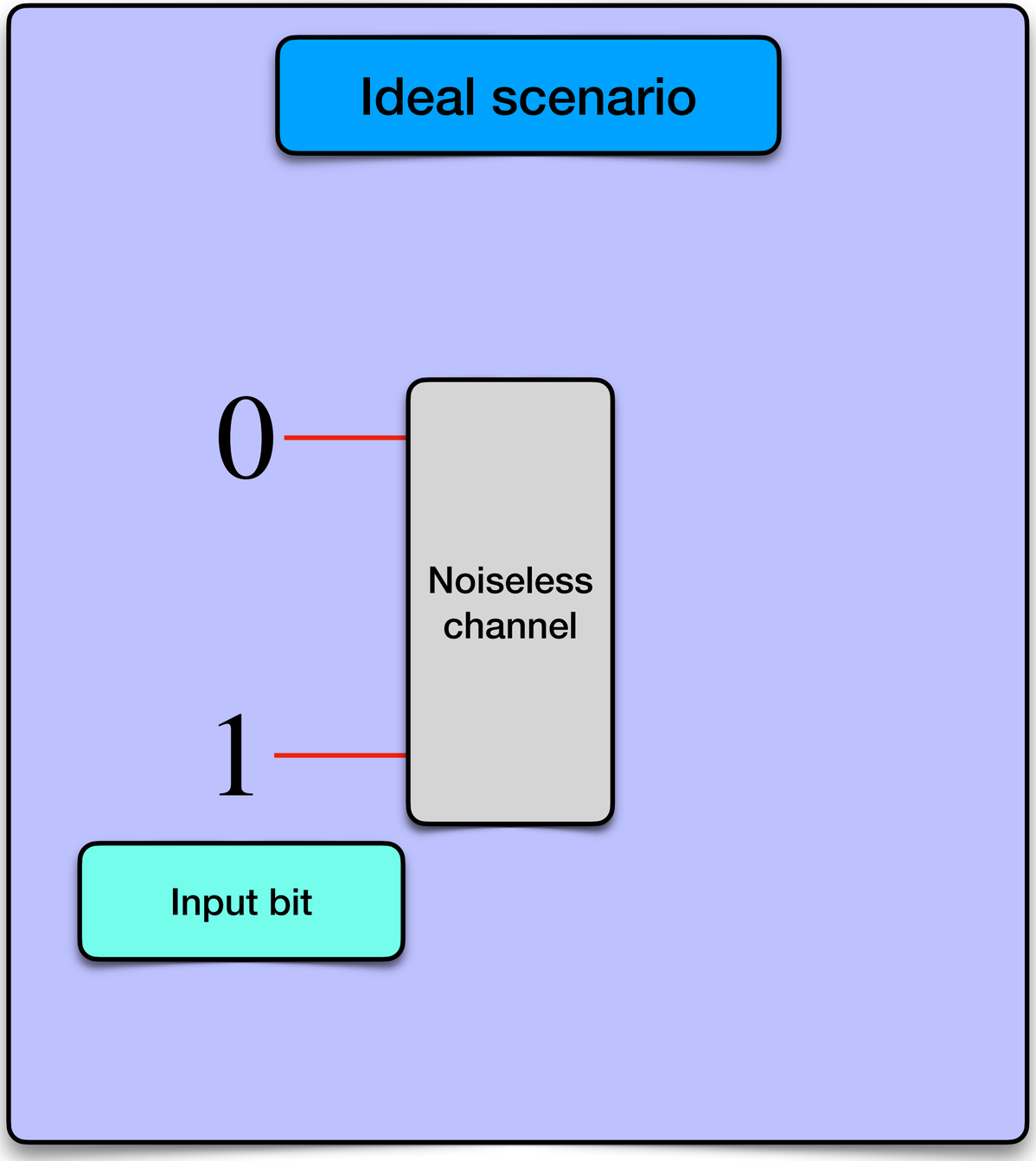
Errors in different circuits

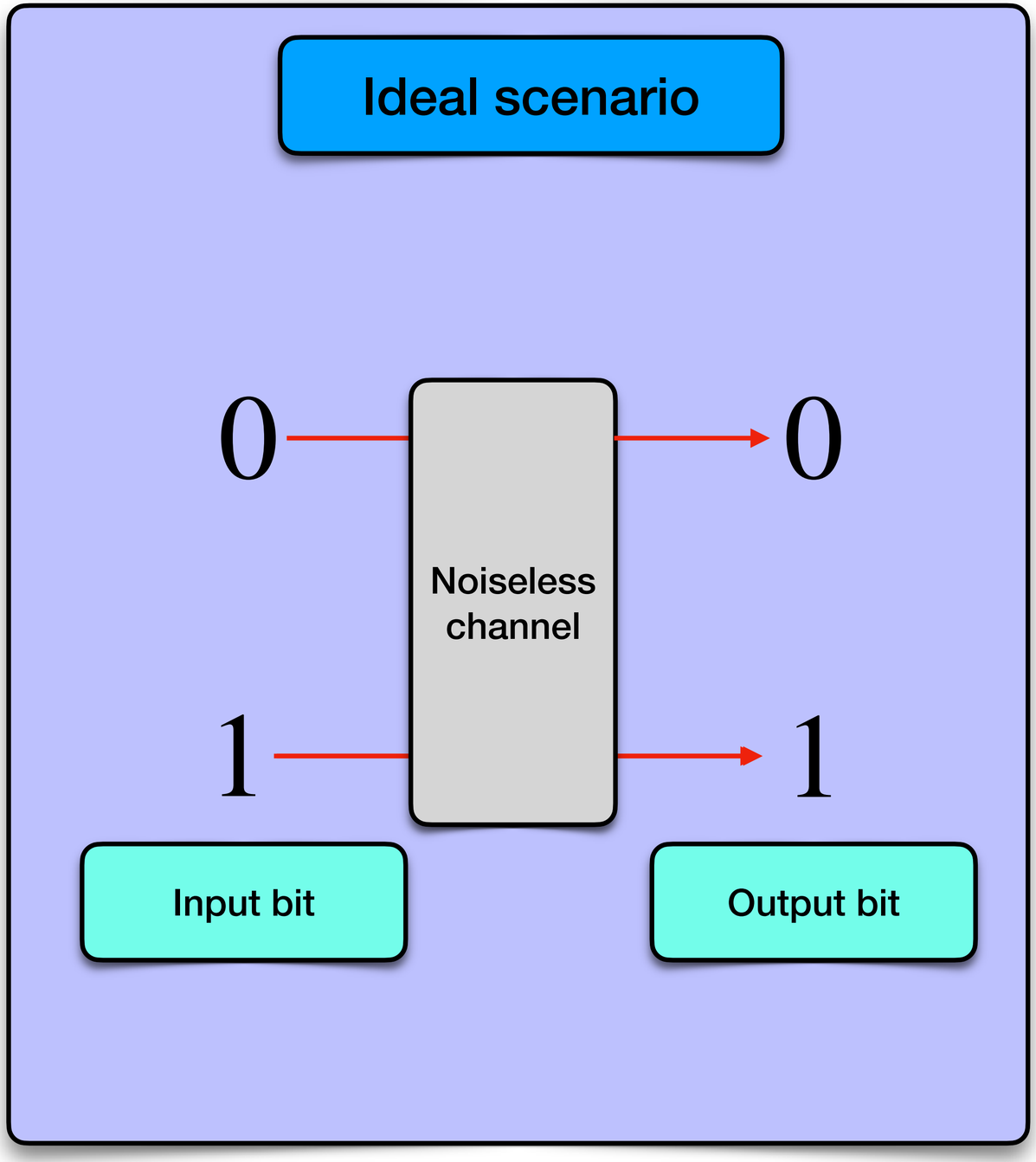
One qubit circuit				
Outcome	$\|0\rangle$	$\|1\rangle$		
Simulation	0.482	0.518		
Experiment	0.538	0.462		
Entangling circuit				
Outcome	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
Simulation	0.495	0	0	0.505
Experiment	0.458	0.047	0.061	0.434
Phase estimator circuit				
Outcome	$\|000\rangle$	$\|001\rangle$	$\|010\rangle$	$\|011\rangle$
Simulation	0.405	0.088	0.077	0.430
Experiment	0.484	0.149	0.033	0.085
Outcome	$\|100\rangle$	$\|101\rangle$	$\|110\rangle$	$\|111\rangle$
Simulation	0	0	0	0
Experiment	0.152	0.055	0.024	0.018

Understanding and compensating for noise on IBM quantum computers

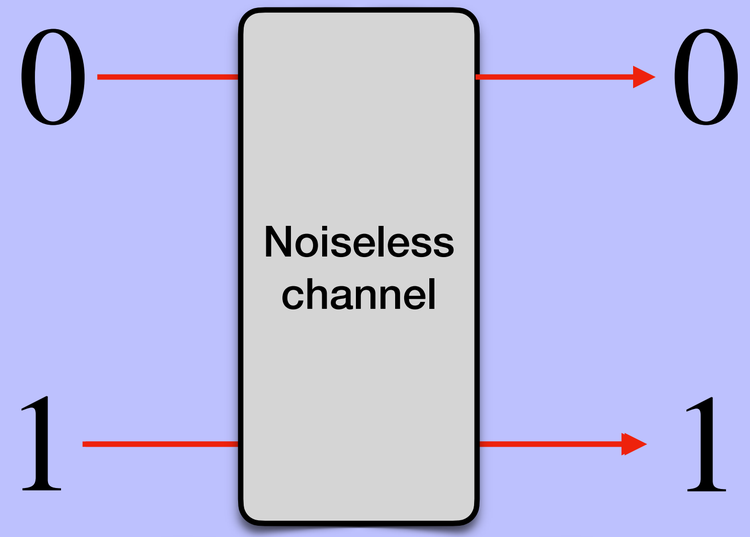
Scott Johnstun and Jean-François Van Huele
American Journal of Physics **89**, 935 (2021)


Ideal scenario
0
1
Input bit


Ideal scenario
0
1
Noiseless channel
Input bit


Ideal scenario
0
1
Noiseless channel
0
1
Input bit
Output bit

Ideal scenario

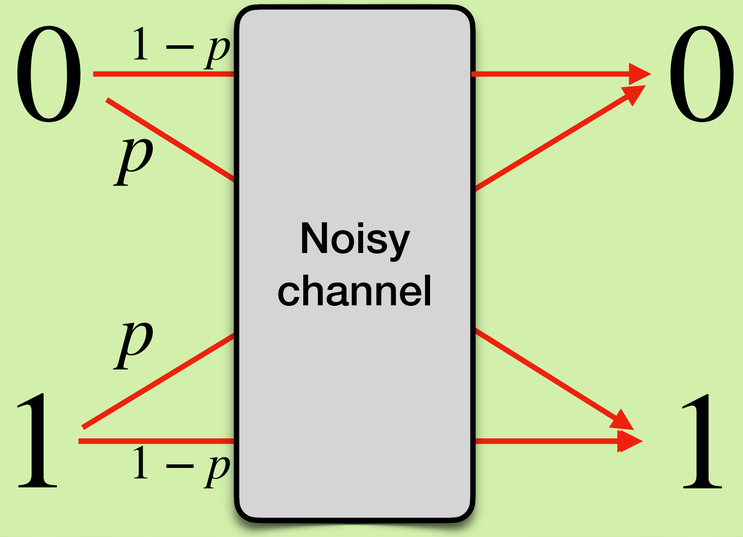


Input bit

Output bit

Model of Realistic situation

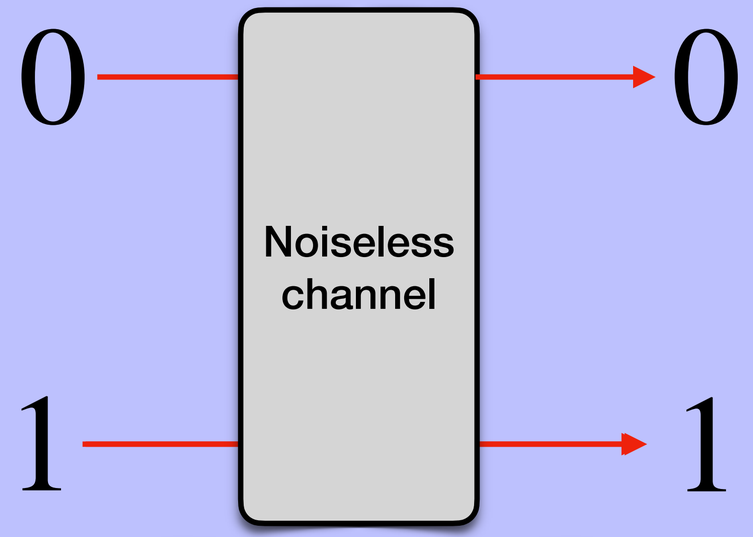
Binary “symmetric” channel



Input bit

Output bit

Ideal scenario

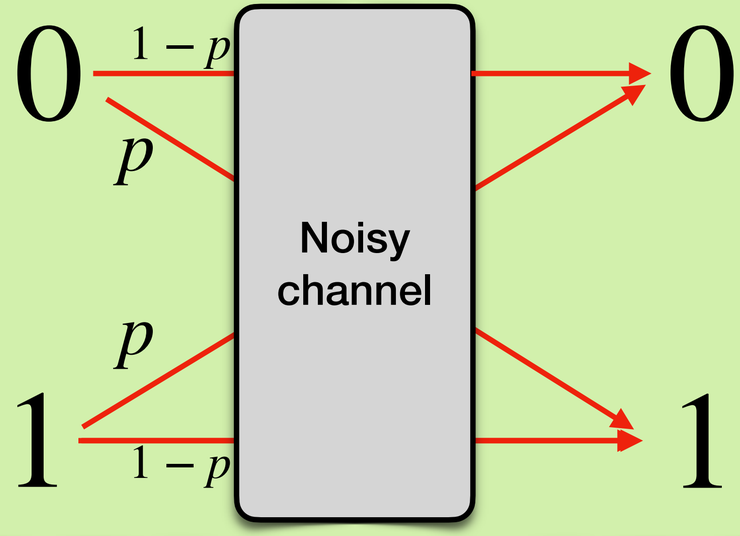


Input bit

Output bit

Model of Realistic situation

Binary “symmetric” channel



Input bit

Output bit

$p << 1$

How to correct these errors?

How to correct these errors?

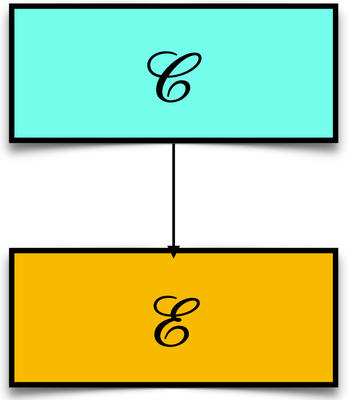
Classical repetition code

Classical repetition code

- **Error Model**
  - Channels provide description of the type of error

$\mathscr{E}$

Classical repetition code

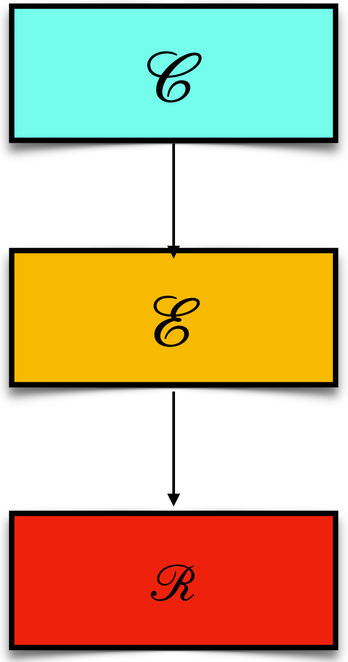


- **Error Model**
  - Channels provide description of the type of error

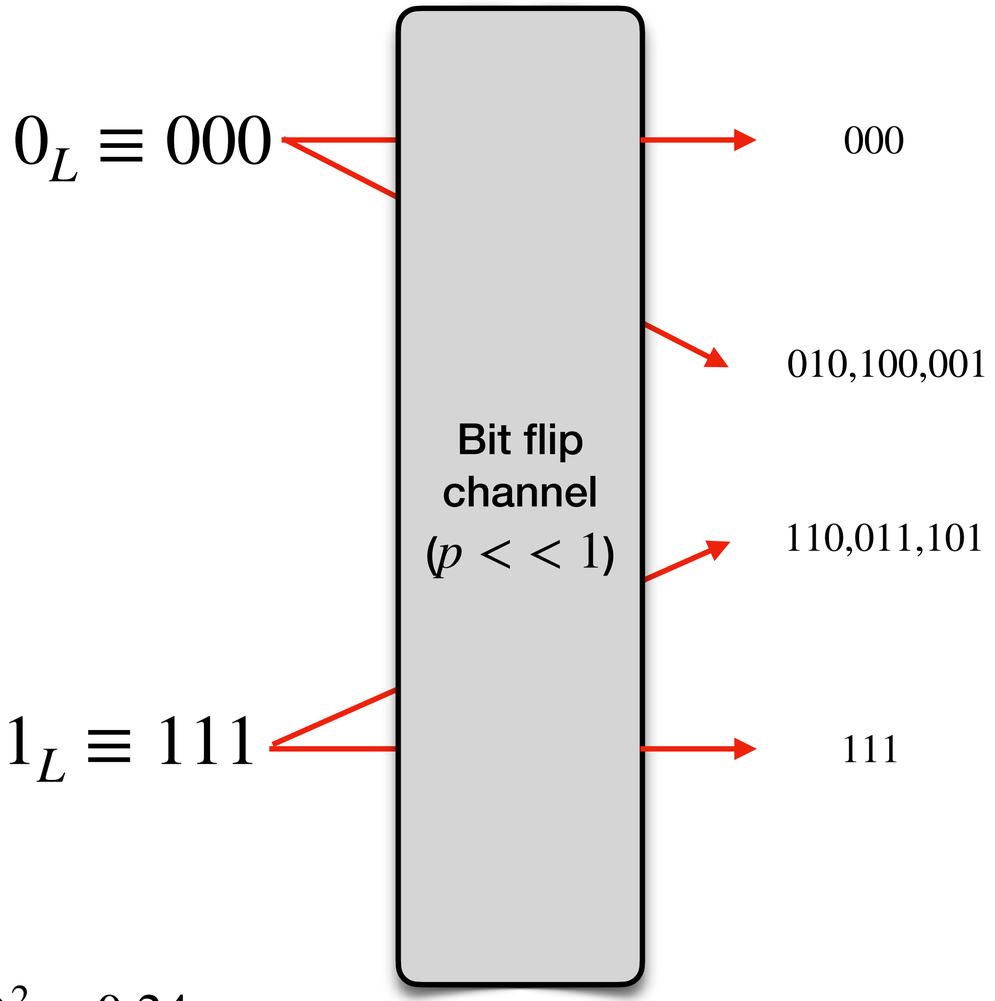
- **Encoding**
  - Extra bits added to protect logical bit
  - String of bits ≡ codeword
  - Redundancy

Classical repetition code

- **Error Model**
  - Channels provide description of the type of error
- **Encoding**
  - Extra bits added to protect logical bit
  - String of bits ≡ codeword
  - Redundancy
- **Error detection and correction**
  - Recovery operation
  - Measure bits and re-set all values to majority vote



An example: Classical repetition code



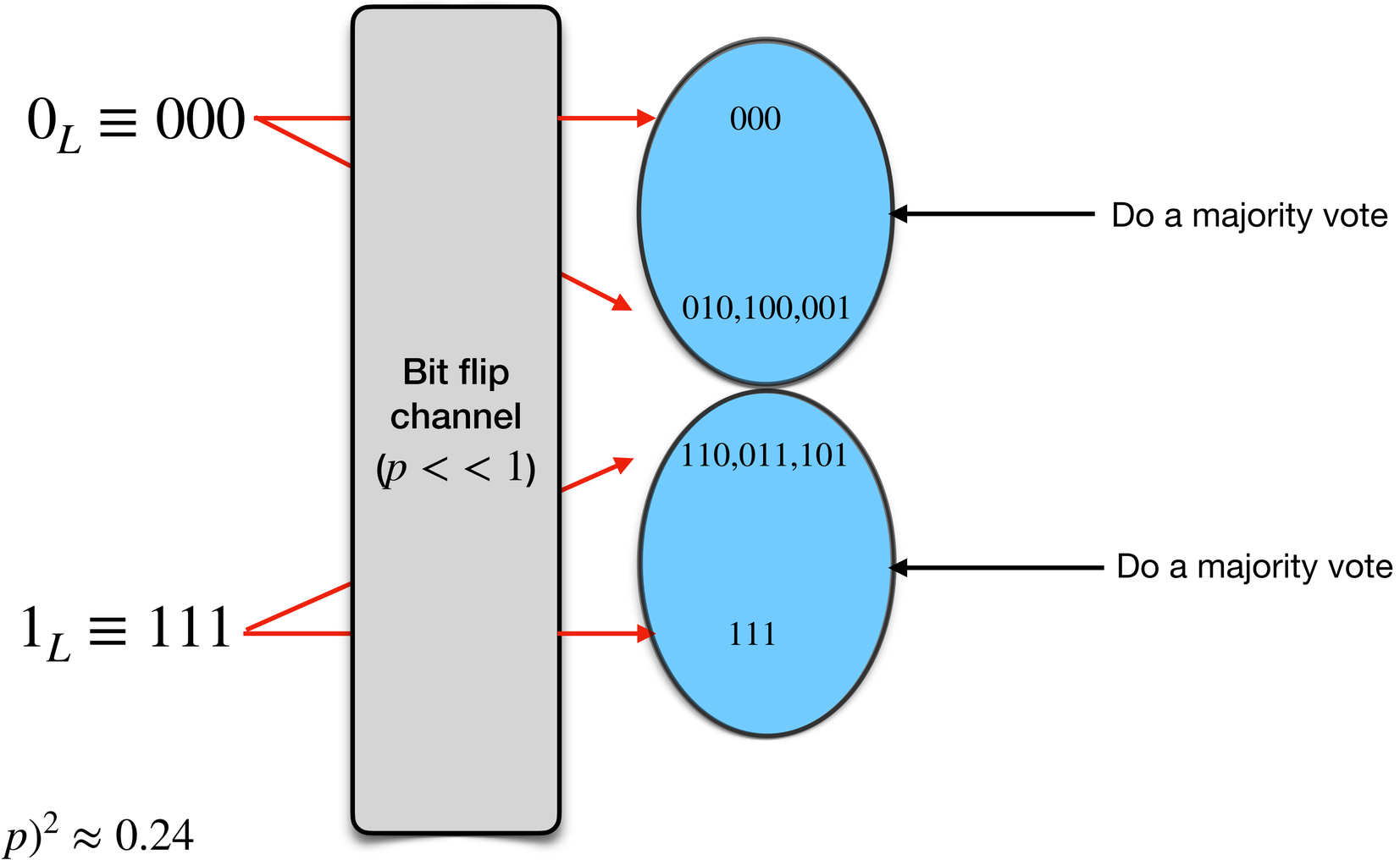
$p = 0.1$

Probability of a single bit flip=$3p(1-p)^2 \approx 0.24$

Probability of two bit flips=$3p^2(1-p) \approx 0.027$

Probability of three bit flips=$p^3 = 0.001$

An example: Classical repetition code



$p = 0.1$

Probability of a single bit flip=$3p(1-p)^2 \approx 0.24$

Probability of two bit flips=$3p^2(1-p) \approx 0.027$

Probability of three bit flips=$p^3 = 0.001$

An example: Classical repetition code

- Corrects a single bit-flip error for classical data

$$0 \rightarrow 000$$
$$1 \rightarrow 111$$

Detection and Correction procedure:

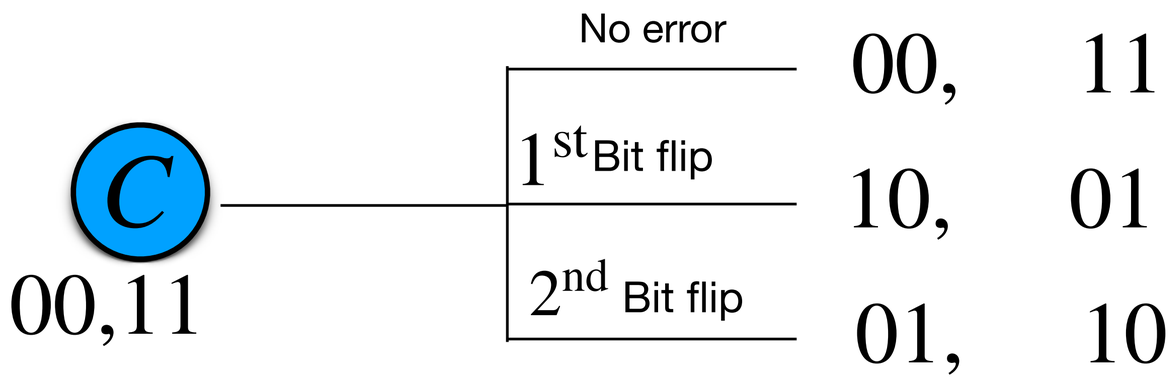
Choose the majority of the three bits, e.g.,

$$010 \rightarrow 0, \quad 101 \rightarrow 1$$

- If error probability is small, one error is more likely than two.

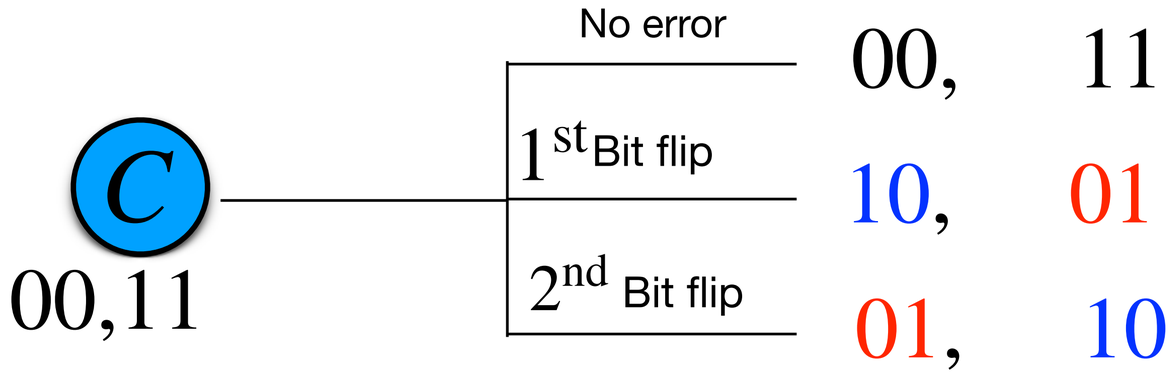
Why three?

Because we want perfect discrimination.



Why three?

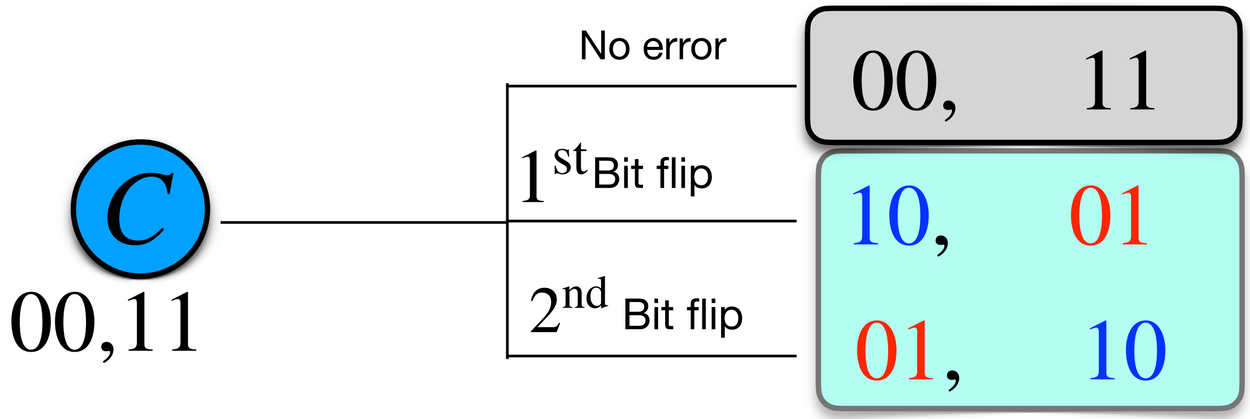
Because we want perfect discrimination.



Cannot distinguish errors!

Why three?

Because we want perfect discrimination.

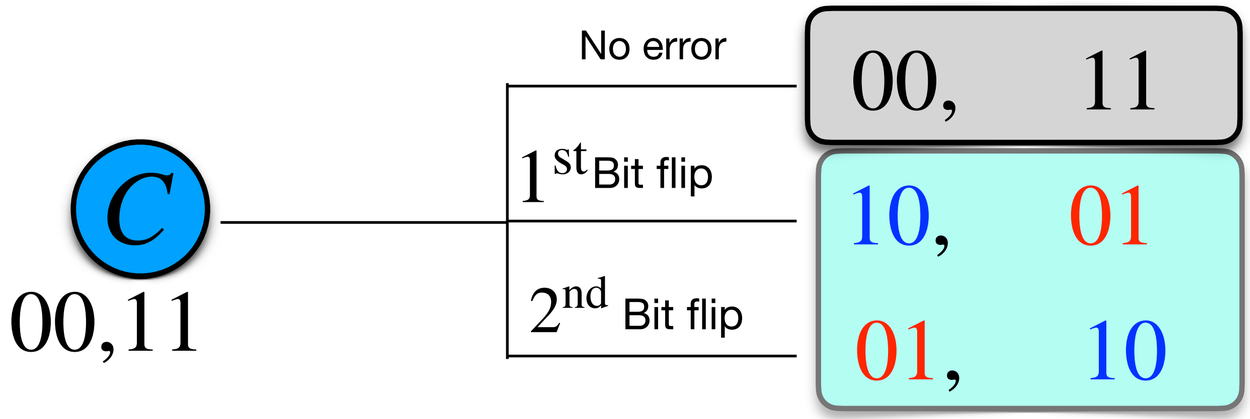


Cannot distinguish errors!

What are we getting?

Why three?

Because we want perfect discrimination.



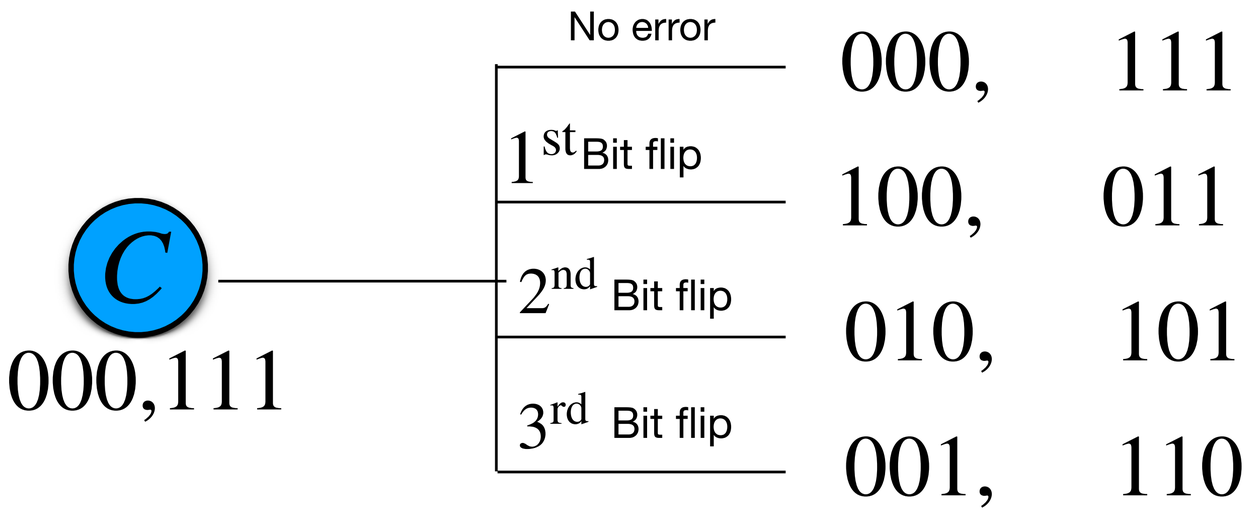
Cannot distinguish errors!

What are we getting?

Whether an error has occurred or not!

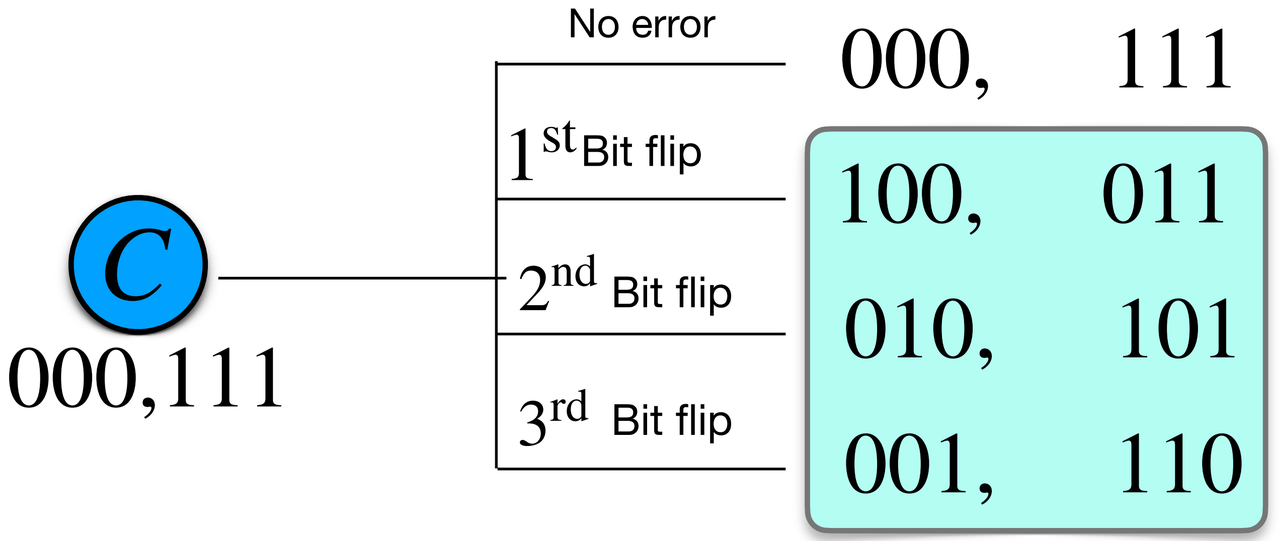
Why three?

Because we want perfect discrimination.



Why three?

Because we want perfect discrimination.



Can distinguish errors!

A bit of details and mathematical formulation:
Classical error-correcting codes

CSS Code [n, k] code

n bits encoding k logical bits

? ?

Generator matrix G: maps messages to their equivalents in code spaces.

Code $\rightarrow y = Gx \leftarrow$ Message

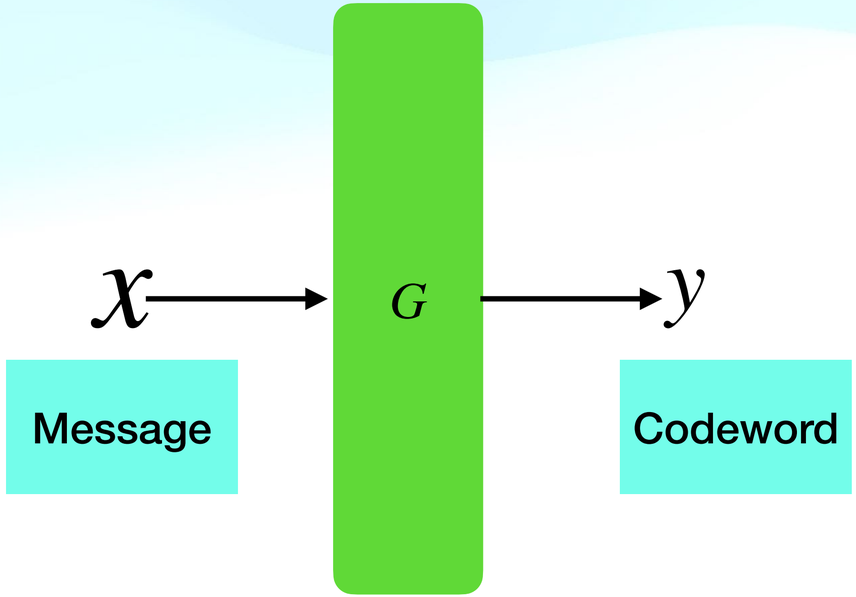
CSS Code [n, k] code

n bits encoding k logical bits

? ?

Generator matrix G: maps messages to their equivalents in code spaces.

Code $\rightarrow y = Gx \leftarrow$ Message



CSS Code [n, k] code

n bits encoding k logical bits

Generator matrix G: maps messages to their equivalents in code spaces.

Code $\rightarrow y = Gx \leftarrow$ Message

Example: $0 \rightarrow (0,0,0)^T$ $1 \rightarrow (1,1,1)^T$

CSS Code [n, k] code

n bits encoding k logical bits

Generator matrix G: maps messages to their equivalents in code spaces.

Code $\rightarrow y = Gx \leftarrow$ Message

$0 \rightarrow (0,0,0)^T$ $\quad$ $1 \rightarrow (1,1,1)^T$

$$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

CSS Code [n, k] code

n bits encoding k logical bits

Generator matrix G: maps messages to their equivalents in code spaces.

Code $\rightarrow y = Gx \leftarrow$ Message

$0 \rightarrow (0,0,0)^T$ $\quad$ $1 \rightarrow (1,1,1)^T$

$$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

Encoding of message

$$G \quad x \quad y$$

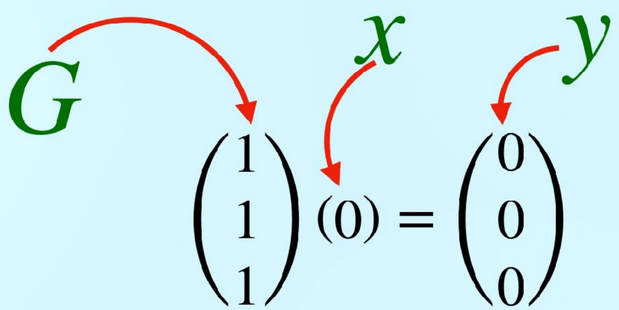
$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} (0) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

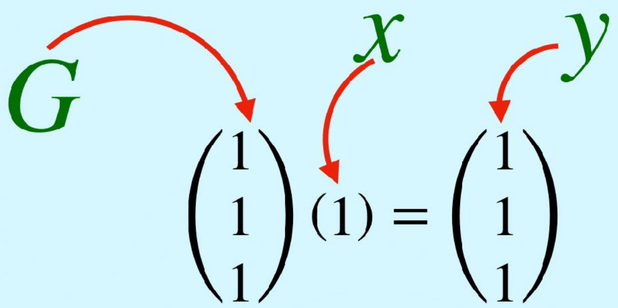
[3,1] code

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} (1) = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

Of what use?

Example: A [3, 1, 1] code



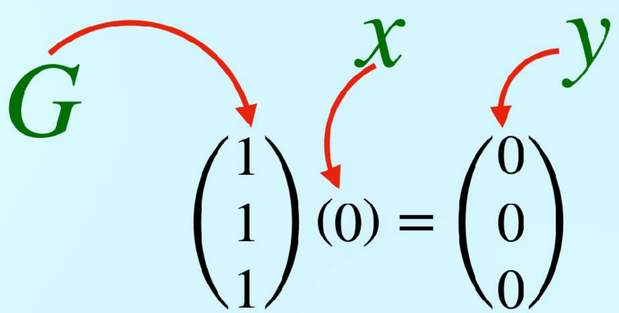


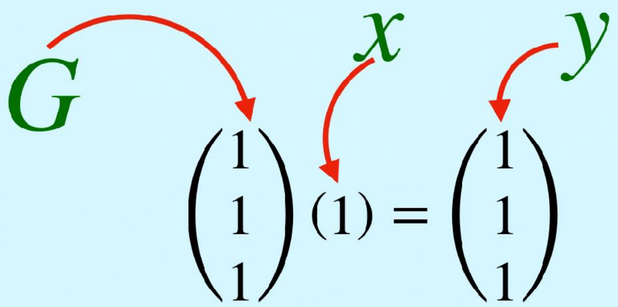
$$\begin{pmatrix}0\\0\\0\end{pmatrix} \rightarrow \begin{pmatrix}1\\0\\0\end{pmatrix}$$

$$\begin{pmatrix}1\\1\\1\end{pmatrix} \rightarrow \begin{pmatrix}0\\1\\1\end{pmatrix}$$

1st bit corrupted

Example: A [3, 1, 1] code





$$\begin{pmatrix}0\\0\\0\end{pmatrix} \to \begin{pmatrix}1\\0\\0\end{pmatrix};$$

$$\begin{pmatrix}1\\1\\1\end{pmatrix} \to \begin{pmatrix}0\\1\\1\end{pmatrix};$$

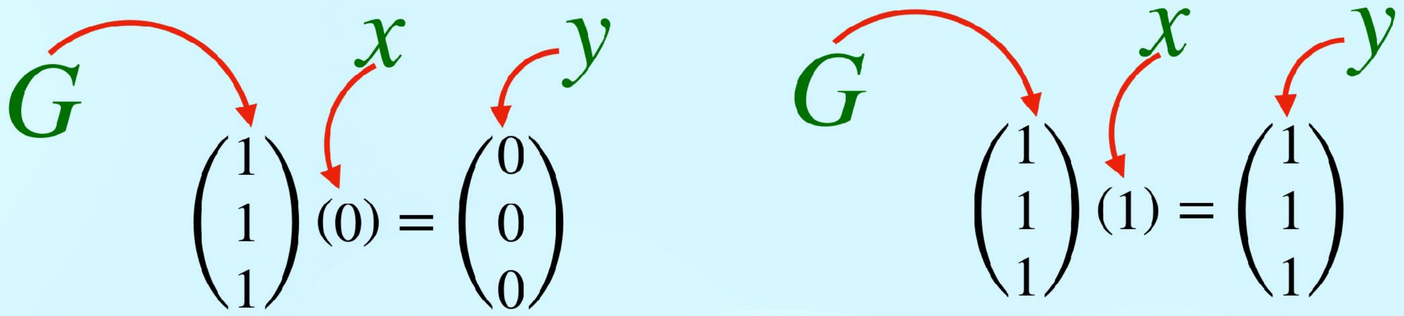
1st bit corrupted

$$\begin{pmatrix}0\\0\\0\end{pmatrix} \to \begin{pmatrix}0\\1\\0\end{pmatrix}$$

$$\begin{pmatrix}1\\1\\1\end{pmatrix} \to \begin{pmatrix}1\\0\\1\end{pmatrix}$$

2nd bit corrupted

Example: A [3, 1, 1] code



$$\begin{pmatrix}0\\0\\0\end{pmatrix} \to \begin{pmatrix}1\\0\\0\end{pmatrix};\quad \begin{pmatrix}1\\1\\1\end{pmatrix} \to \begin{pmatrix}0\\1\\1\end{pmatrix};$$

1st bit corrupted

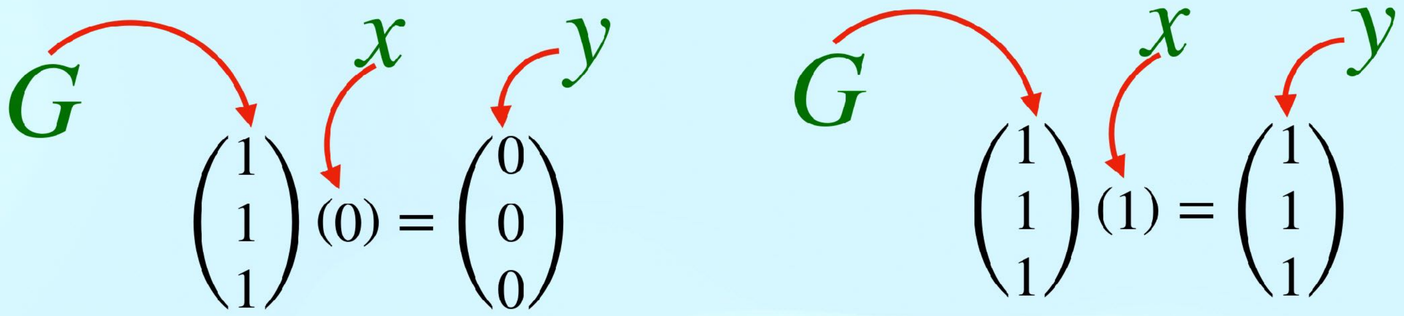
$$\begin{pmatrix}0\\0\\0\end{pmatrix} \to \begin{pmatrix}0\\1\\0\end{pmatrix};\quad \begin{pmatrix}1\\1\\1\end{pmatrix} \to \begin{pmatrix}1\\0\\1\end{pmatrix};$$

2nd bit corrupted

$$\begin{pmatrix}0\\0\\0\end{pmatrix} \to \begin{pmatrix}0\\0\\1\end{pmatrix};\quad \begin{pmatrix}1\\1\\1\end{pmatrix} \to \begin{pmatrix}1\\1\\0\end{pmatrix}$$

3rd bit corrupted

Example: A [3, 1, 1] code



$$\begin{pmatrix}0\\0\\0\end{pmatrix} \to \begin{pmatrix}1\\0\\0\end{pmatrix}; \quad \begin{pmatrix}1\\1\\1\end{pmatrix} \to \begin{pmatrix}0\\1\\1\end{pmatrix};$$

1st bit corrupted

$$\begin{pmatrix}0\\0\\0\end{pmatrix} \to \begin{pmatrix}0\\1\\0\end{pmatrix}; \quad \begin{pmatrix}1\\1\\1\end{pmatrix} \to \begin{pmatrix}1\\0\\1\end{pmatrix};$$

2nd bit corrupted

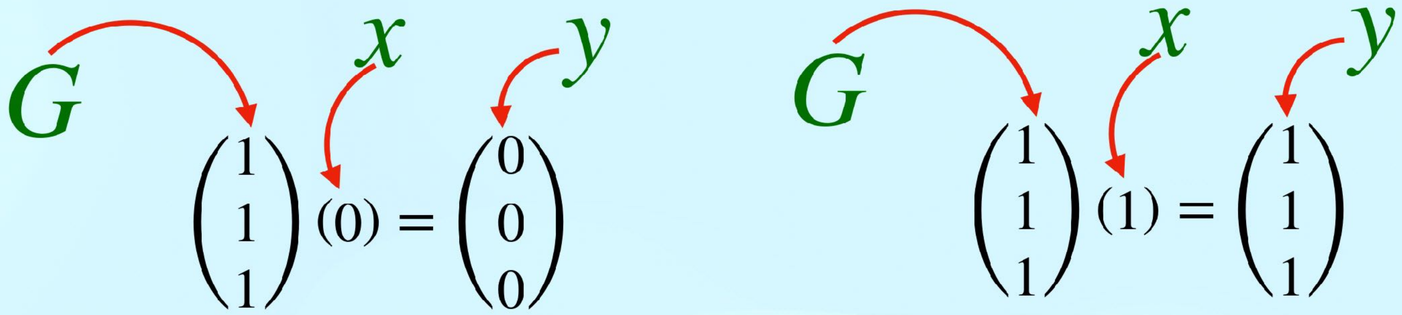
$$\begin{pmatrix}0\\0\\0\end{pmatrix} \to \begin{pmatrix}0\\0\\1\end{pmatrix}; \quad \begin{pmatrix}1\\1\\1\end{pmatrix} \to \begin{pmatrix}1\\1\\0\end{pmatrix};$$

3rd bit corrupted

$$\begin{pmatrix}0\\0\\0\end{pmatrix} \to \begin{pmatrix}0\\0\\0\end{pmatrix}; \quad \begin{pmatrix}1\\1\\1\end{pmatrix} \to \begin{pmatrix}1\\1\\1\end{pmatrix};$$

No error

Example: A [3, 1, 1] code



Can you identify a pattern?

$\begin{pmatrix}0\\0\\0\end{pmatrix}\rightarrow\begin{pmatrix}1\\0\\0\end{pmatrix}$; $\begin{pmatrix}1\\1\\1\end{pmatrix}\rightarrow\begin{pmatrix}0\\1\\1\end{pmatrix}$;

1st bit corrupted

$\begin{pmatrix}0\\0\\0\end{pmatrix}\rightarrow\begin{pmatrix}0\\1\\0\end{pmatrix}$; $\begin{pmatrix}1\\1\\1\end{pmatrix}\rightarrow\begin{pmatrix}1\\0\\1\end{pmatrix}$;

2nd bit corrupted

$\begin{pmatrix}0\\0\\0\end{pmatrix}\rightarrow\begin{pmatrix}0\\0\\1\end{pmatrix}$; $\begin{pmatrix}1\\1\\1\end{pmatrix}\rightarrow\begin{pmatrix}1\\1\\0\end{pmatrix}$;

3rd bit corrupted

$\begin{pmatrix}0\\0\\0\end{pmatrix}\rightarrow\begin{pmatrix}0\\0\\0\end{pmatrix}$ $\begin{pmatrix}1\\1\\1\end{pmatrix}\rightarrow\begin{pmatrix}1\\1\\1\end{pmatrix}$

No error

Example: A [3, 1, 1] code

$$G \quad x \quad y$$

$$\begin{pmatrix}1\\1\\1\end{pmatrix}(0) = \begin{pmatrix}0\\0\\0\end{pmatrix}$$

$$G \quad x \quad y$$

$$\begin{pmatrix}1\\1\\1\end{pmatrix}(1) = \begin{pmatrix}1\\1\\1\end{pmatrix}$$

Can you identify a pattern?

Do a bit-wise addition.

$$\begin{pmatrix}0\\0\\0\end{pmatrix} \to \begin{pmatrix}1\\0\\0\end{pmatrix}; \quad \begin{pmatrix}1\\1\\1\end{pmatrix} \to \begin{pmatrix}0\\1\\1\end{pmatrix};$$

1st bit corrupted

$$\begin{pmatrix}0\\0\\0\end{pmatrix} \to \begin{pmatrix}0\\1\\0\end{pmatrix}; \quad \begin{pmatrix}1\\1\\1\end{pmatrix} \to \begin{pmatrix}1\\0\\1\end{pmatrix};$$

2nd bit corrupted

$$\begin{pmatrix}0\\0\\0\end{pmatrix} \to \begin{pmatrix}0\\0\\1\end{pmatrix}; \quad \begin{pmatrix}1\\1\\1\end{pmatrix} \to \begin{pmatrix}1\\1\\0\end{pmatrix};$$

3rd bit corrupted

$$\begin{pmatrix}0\\0\\0\end{pmatrix} \to \begin{pmatrix}0\\0\\0\end{pmatrix}; \quad \begin{pmatrix}1\\1\\1\end{pmatrix} \to \begin{pmatrix}1\\1\\1\end{pmatrix};$$

No error

On the first two bits.

On the last two bits.

Example: A [3, 1, 1] code

$$G \xrightarrow{x} \begin{pmatrix}1\\1\\1\end{pmatrix} \xrightarrow{(0)} = \begin{pmatrix}0\\0\\0\end{pmatrix} \xrightarrow{y}$$

$$G \xrightarrow{x} \begin{pmatrix}1\\1\\1\end{pmatrix} \xrightarrow{(1)} = \begin{pmatrix}1\\1\\1\end{pmatrix} \xrightarrow{y}$$

Can you identify a pattern?

Do a bit-wise addition.

1st bit corrupted	2nd bit corrupted	3rd bit corrupted	No error
$\begin{pmatrix}0\\0\\0\end{pmatrix} \to \begin{pmatrix}1\\0\\0\end{pmatrix}$;	$\begin{pmatrix}0\\0\\0\end{pmatrix} \to \begin{pmatrix}0\\1\\0\end{pmatrix}$;	$\begin{pmatrix}0\\0\\0\end{pmatrix} \to \begin{pmatrix}0\\0\\1\end{pmatrix}$;	$\begin{pmatrix}0\\0\\0\end{pmatrix} \to \begin{pmatrix}0\\0\\0\end{pmatrix}$
$\begin{pmatrix}1\\1\\1\end{pmatrix} \to \begin{pmatrix}0\\1\\1\end{pmatrix}$;	$\begin{pmatrix}1\\1\\1\end{pmatrix} \to \begin{pmatrix}1\\0\\1\end{pmatrix}$;	$\begin{pmatrix}1\\1\\1\end{pmatrix} \to \begin{pmatrix}1\\1\\0\end{pmatrix}$;	$\begin{pmatrix}1\\1\\1\end{pmatrix} \to \begin{pmatrix}1\\1\\1\end{pmatrix}$

On the first two bits.

On the last two bits.

Can you differentiate among all?

Error detection

CSS Code [n, k] code

n bits encoding k logical bits

Generator matrix G: maps messages to their equivalents in code spaces.

Code $\rightarrow y = Gx \leftarrow$ Message

$0 \rightarrow (0,0,0)^T$ $\quad$ $1 \rightarrow (1,1,1)^T$

$$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

$$Hy = 0$$

$(n-k) \times n$ Matrix with entries in $\{0,1\}$

Parity check matrix

CSS Code [n, k] code

n bits encoding k logical bits

Generator matrix G: maps messages to their equivalents in code spaces.

Code $\rightarrow y = Gx \leftarrow$ Message

$0 \rightarrow (0,0,0)^T$ $\quad$ $1 \rightarrow (1,1,1)^T$

$$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

$Hy = 0$

$(n-k) \times n$ Matrix with entries in $\{0,1\}$

Parity check matrix

$(n-k)$ Linearly independent vectors orthogonal to the columns of G.

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

CSS Code [n, k] code

n bits encoding k logical bits

Generator matrix G: maps messages to their equivalents in code spaces.

Code $\rightarrow y = Gx \leftarrow$ Message

$0 \rightarrow (0,0,0)^T$ $\quad$ $1 \rightarrow (1,1,1)^T$

$$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

$$Hy = 0$$

$(n-k) \times n$ Matrix with entries in $\{0,1\}$

$(n-k)$ Linearly independent vectors orthogonal to the columns of G.

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

$1 \cdot 1 + 1 \cdot 1 + 1 \cdot 0 \equiv 0$

CSS Code [n, k] code

n bits encoding k logical bits

Generator matrix G: maps messages to their equivalents in code spaces.

Code $\rightarrow y = Gx \leftarrow$ Message

$0 \rightarrow (0,0,0)^T$ $\quad$ $1 \rightarrow (1,1,1)^T$

$$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

$$Hy = 0$$

$(n-k) \times n$ Matrix with entries in $\{0,1\}$

$(n-k)$ Linearly independent vectors orthogonal to the columns of G.

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

$0 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 \equiv 0$

error $e \implies y' \to y + e$

Since $Hy = 0$ for all codewords $y \implies$

$Hy' = Hy + He = He \leftarrow$ Error syndrome

With the help of these error syndromes, we detect the errors and then correct them.

Error detection

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

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

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

NO Error.

Error detection

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

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

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

NO Error.

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

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

Flip on the first bit

Error detection

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

$$\underbrace{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}}_{H} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \qquad \underbrace{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}}_{H} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \longleftarrow$$ NO Error.

$$\underbrace{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}}_{H} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \underbrace{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}}_{H} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \longleftarrow$$ Flip on the first bit.

$$\underbrace{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}}_{H} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad \underbrace{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}}_{H} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \longleftarrow$$ Flip on the second bit.

Error detection

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

NO Error.

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

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

Flip on the first bit.

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

Flip on the third bit.

Flip on the second bit.

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

Classical repetition code
Summary

- Take a message bit.

Classical repetition code
Summary

- Take a message bit.
- Construct a generator matrix G.

Classical repetition code
Summary

- Take a message bit.
- Construct a generator matrix G.
- Find the logical bit.

Classical repetition code
Summary

- Take a message bit.
- Construct a generator matrix G.
- Find the logical bit.
- Construct a parity check matrix H .

Classical repetition code
Summary

- Take a message bit.
- Construct a generator matrix G.
- Find the logical bit.
- Construct a parity check matrix H .
- Find the syndromes.

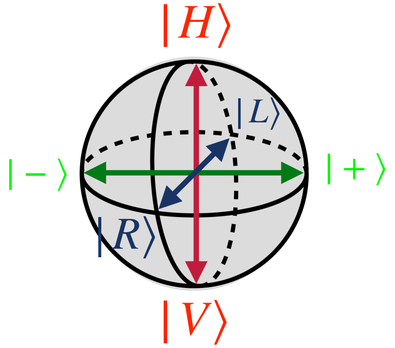
Classical repetition code
Summary

- Take a message bit.
- Construct a generator matrix G.
- Find the logical bit.
- Construct a parity check matrix H .
- Find the syndromes.
- Correct errors.

Question: Construct generator matrix and parity check matrix for a two bit code.

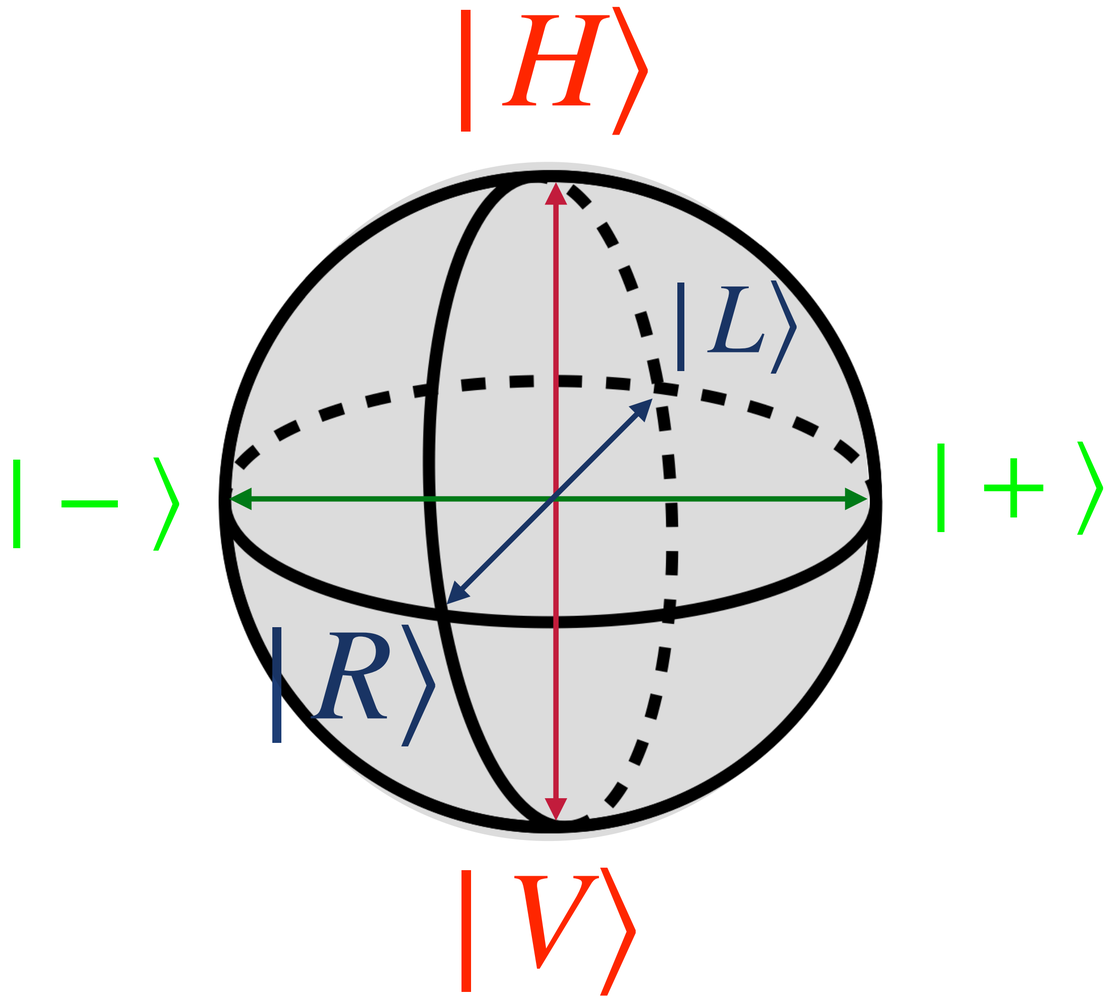
PAUSE

Questions??



What is the situation in the quantum domain?

Qubits: Bloch sphere



Superposition allowed

$$|\pm\rangle = \frac{1}{\sqrt{2}}\Big(|H\rangle \pm |V\rangle\Big)$$

$$|L\rangle = \frac{1}{\sqrt{2}}\Big(|H\rangle + i|V\rangle\Big)$$

$$|R\rangle = \frac{1}{\sqrt{2}}\Big(|H\rangle - i|V\rangle\Big)$$

Single bit flips

$$|0\rangle \rightarrow |1\rangle$$

$$|1\rangle \rightarrow |0\rangle$$

Single bit flips

$$|0\rangle \rightarrow |1\rangle$$

$$|1\rangle \rightarrow |0\rangle$$

AND

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|1\rangle + \beta|0\rangle$$

Is a trivial extension of classical repetition code possible?

For all

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

Is a trivial extension of classical repetition code possible?

For all

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

Answer: NO!!!

Classical Xerox machine

$$00 \rightarrow 00$$

Blank paper

$$10 \rightarrow 11$$

Blank paper

Classical Xerox machine

$00 \rightarrow 00$

Blank paper

$10 \rightarrow 11$

Blank paper

No-Cloning theorem

$$U|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle \qquad U|1\rangle|0\rangle \rightarrow |1\rangle|1\rangle$$

No-Cloning theorem

$$U|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle \qquad U|1\rangle|0\rangle \rightarrow |1\rangle|1\rangle$$

$$U(\alpha|0\rangle + \beta|1\rangle)|0\rangle \rightarrow ?$$

No-Cloning theorem

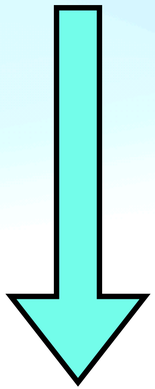
$$U|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle \qquad U|1\rangle|0\rangle \rightarrow |1\rangle|1\rangle$$

$$U(\alpha|0\rangle + \beta|1\rangle)|0\rangle \rightarrow \alpha|00\rangle + \beta|11\rangle \neq (\alpha|0\rangle + \beta|1\rangle)^{\otimes 2}$$

No-Cloning theorem

$$U|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle \qquad U|1\rangle|0\rangle \rightarrow |1\rangle|1\rangle$$

$$U(\alpha|0\rangle + \beta|1\rangle)|0\rangle \rightarrow \alpha|00\rangle + \beta|11\rangle \neq (\alpha|0\rangle + \beta|1\rangle)^{\otimes 2}$$



A trivial extension of repetition code is not possible.

Is it even needed?

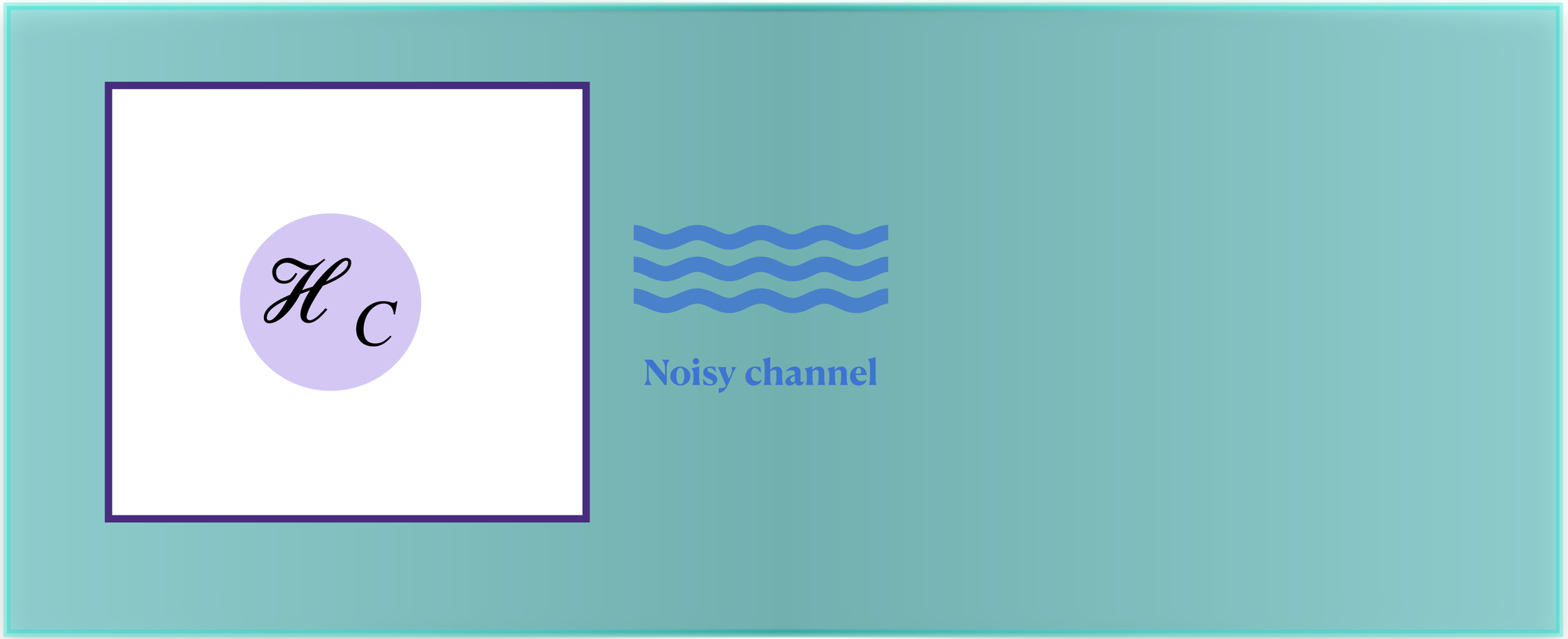
Is it even needed?

NO!!!

Quantum error correcting codes: Basic idea

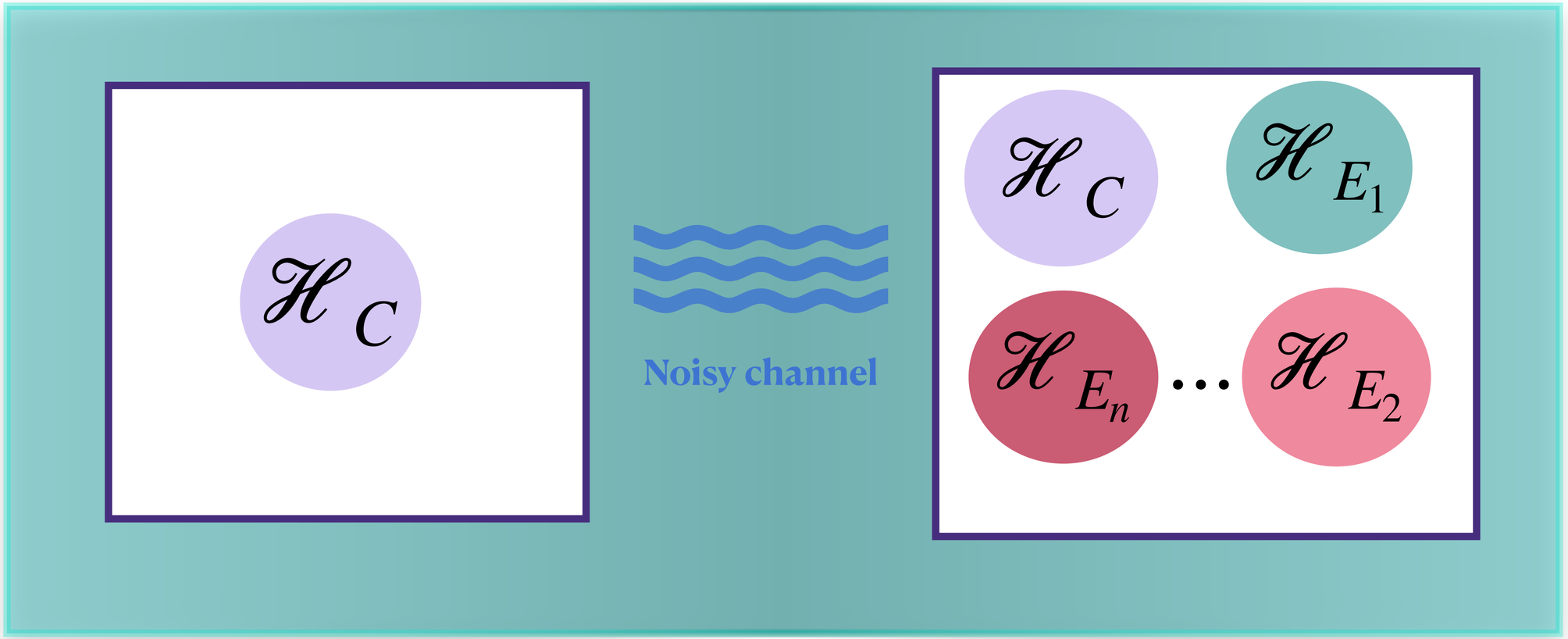
$\mathcal{H}_C$: code space

Quantum error correcting codes: Basic idea



$\mathcal{H}_C$: code space

Quantum error correcting codes: Basic idea

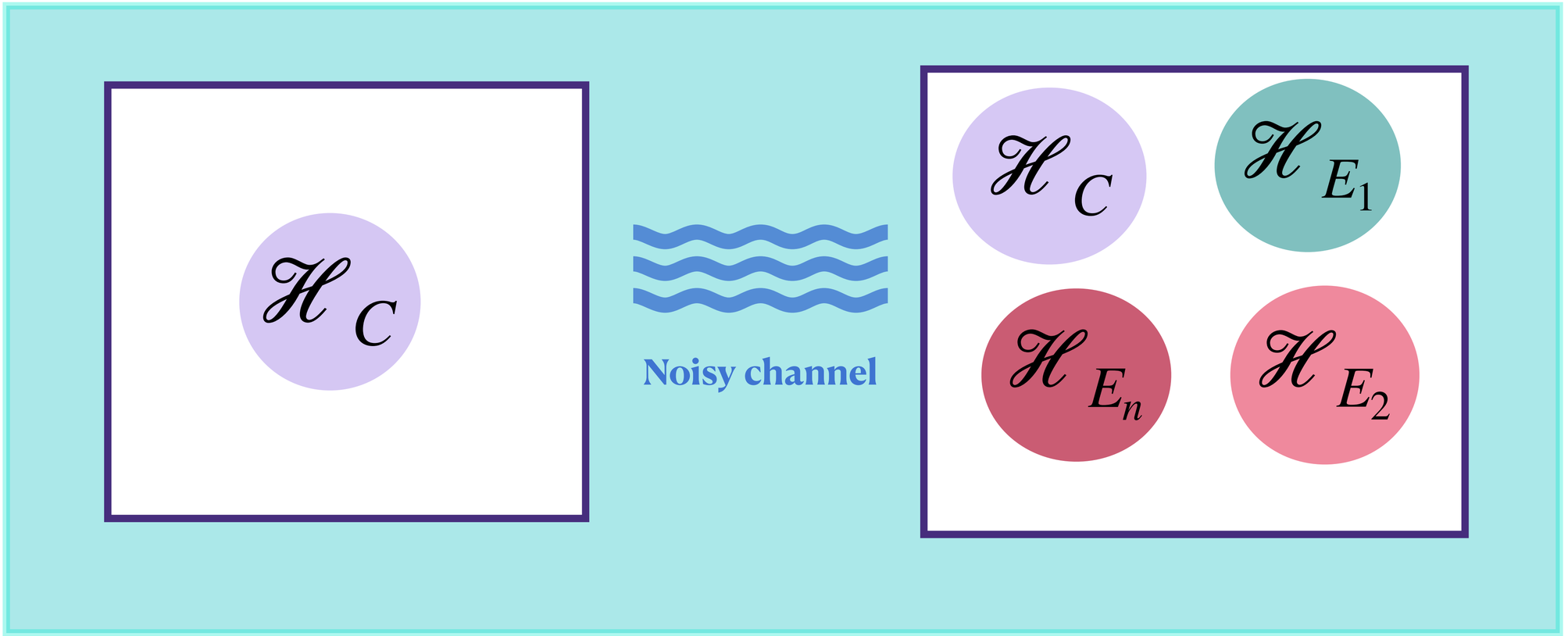


$\mathcal{H}_C$: code space

$\mathcal{H}_{E_i}$: error space

Quantum error correcting codes: Basic idea

$$\mathcal{H}_C \perp \mathcal{H}_{E_1} \perp \mathcal{H}_{E_2} \perp \cdots \perp \mathcal{H}_{E_n}$$

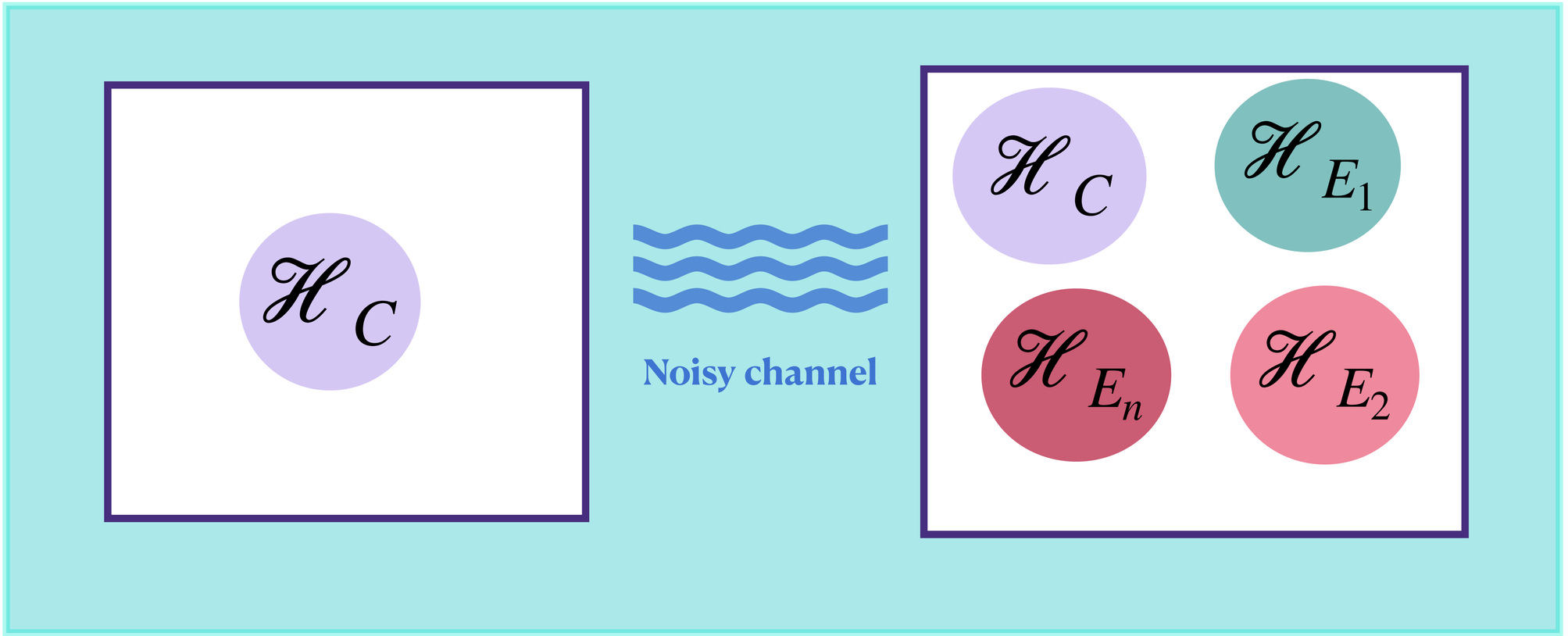


$\mathcal{H}_C$: code space

$\mathcal{H}_{E_i}$: error space

Quantum error correcting codes: Basic idea

$$\mathcal{H}_C \perp \mathcal{H}_{E_1} \perp \mathcal{H}_{E_2} \perp \cdots \perp \mathcal{H}_{E_n}$$



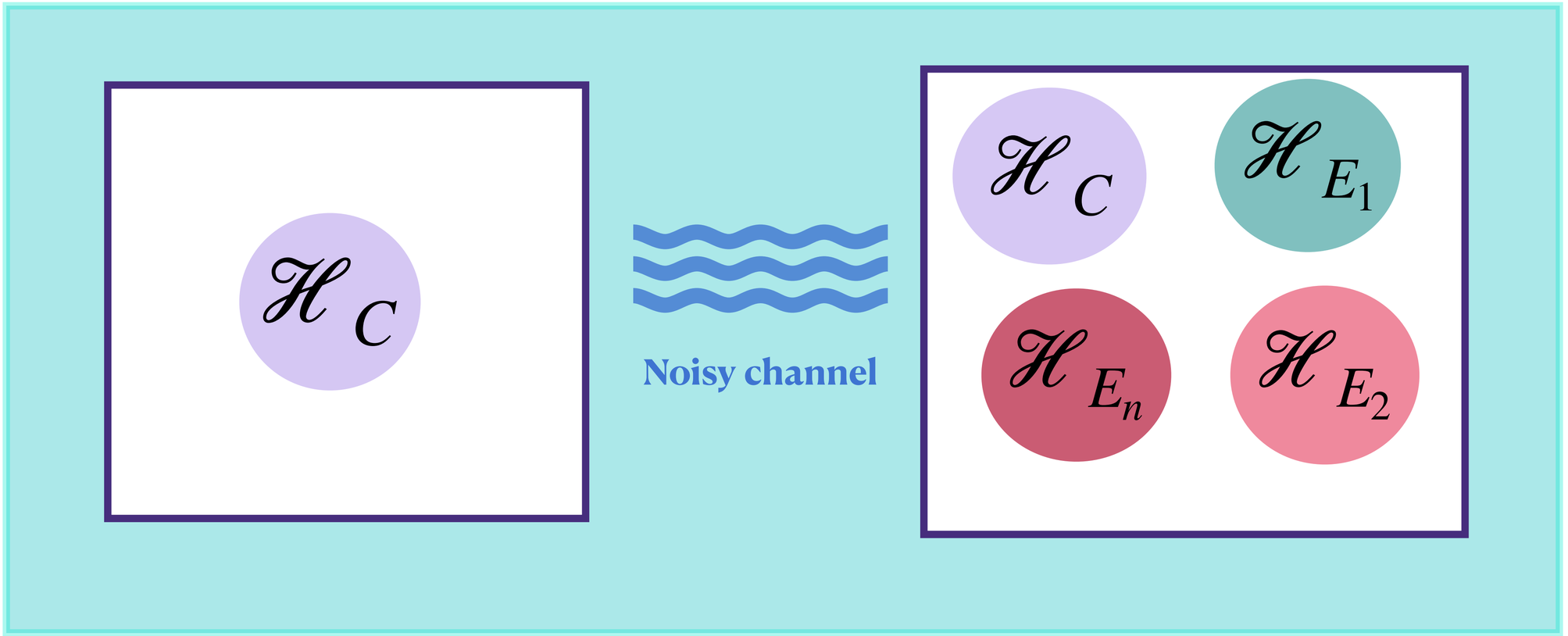
$\mathcal{H}_C$: code space

$\mathcal{H}_{E_i}$: error space

1. Encoding
2. Detection
3. Correction

Quantum error correcting codes: Basic idea

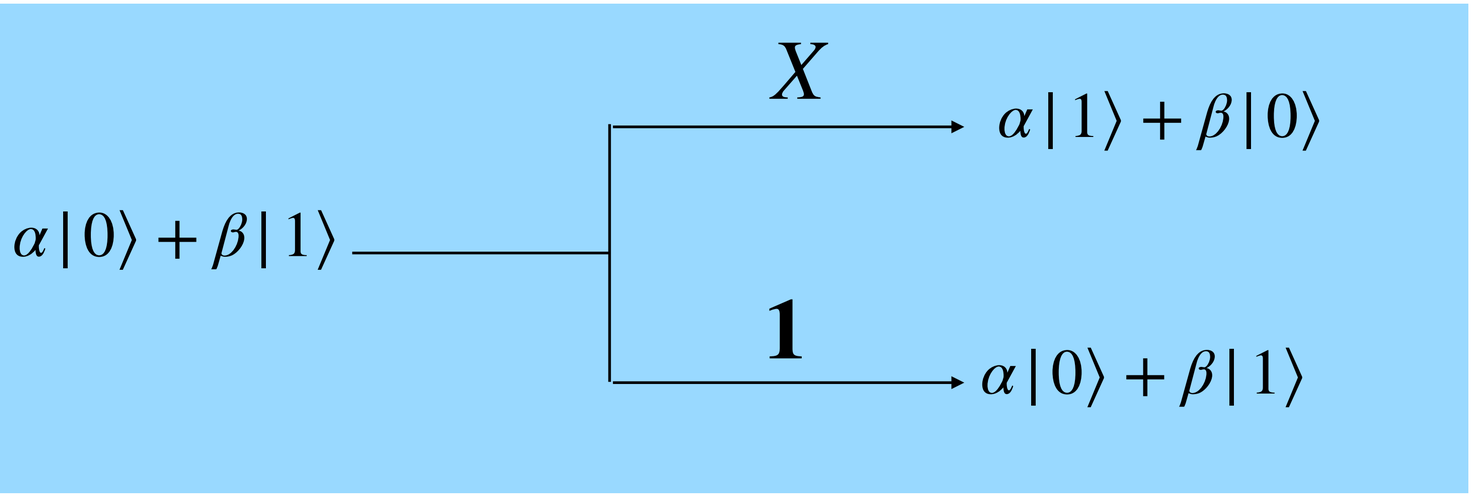
$$\mathcal{H}_C \perp \mathcal{H}_{E_1} \perp \mathcal{H}_{E_2} \perp \cdots \perp \mathcal{H}_{E_n}$$



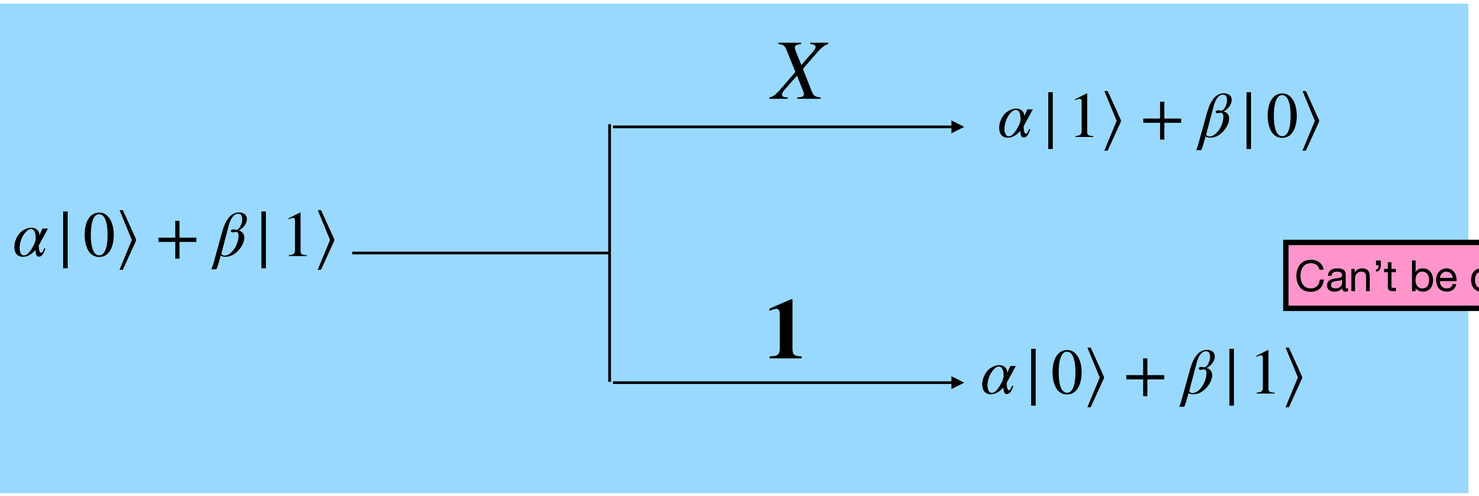
$\mathcal{H}_C$: code space

$\mathcal{H}_{E_i}$: error space

But how?



$$X = |0\rangle\langle 1| + |1\rangle\langle 0|$$



Can’t be distinguished $\alpha^*\beta \neq 0$

Add “enough” ancillary qubits.

Orthogonal states can be unambiguously discriminated by measurement of a hermitian operator.

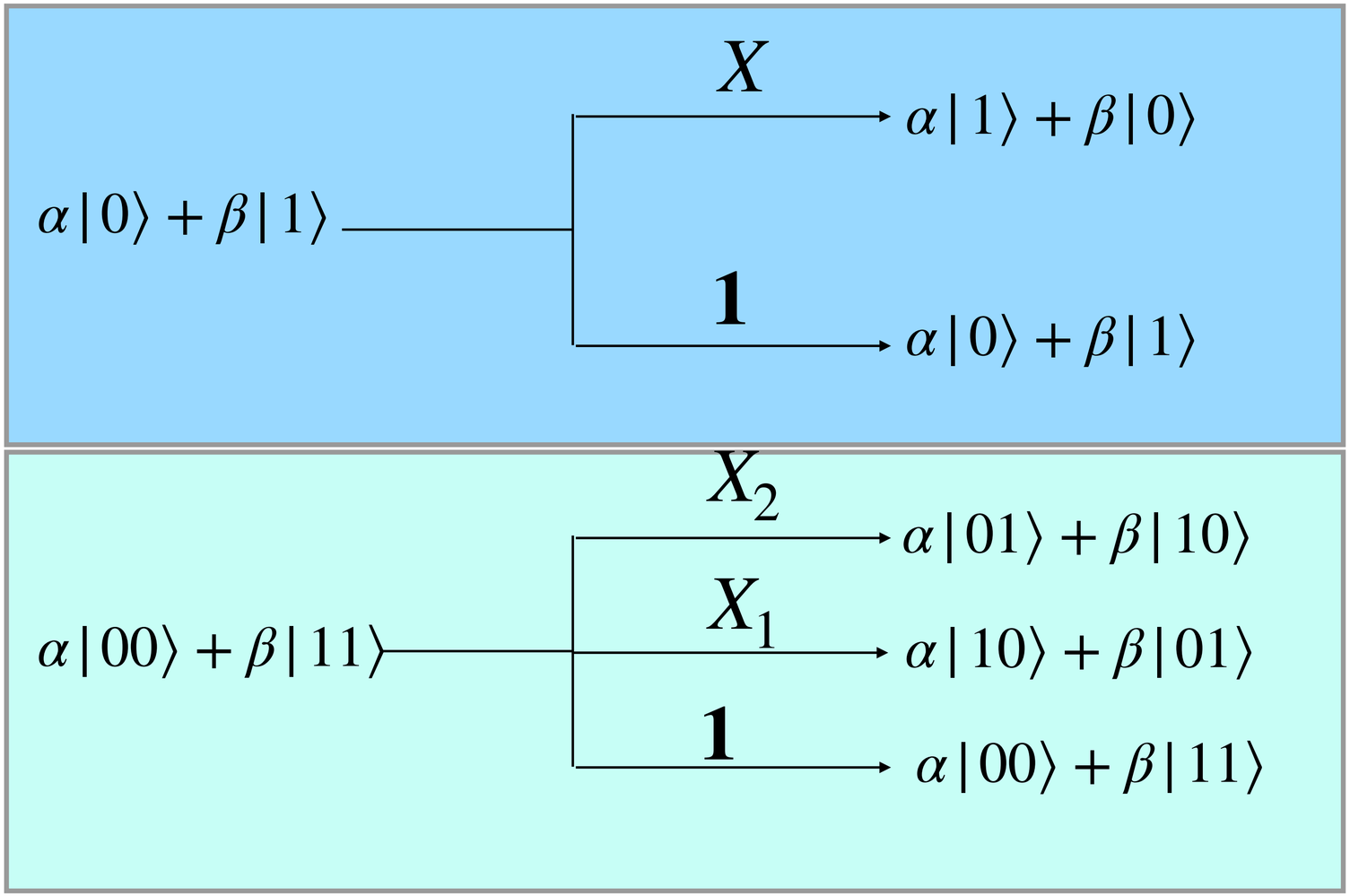
Orthogonal states can be unambiguously discriminated by measurement of a hermitian operator.

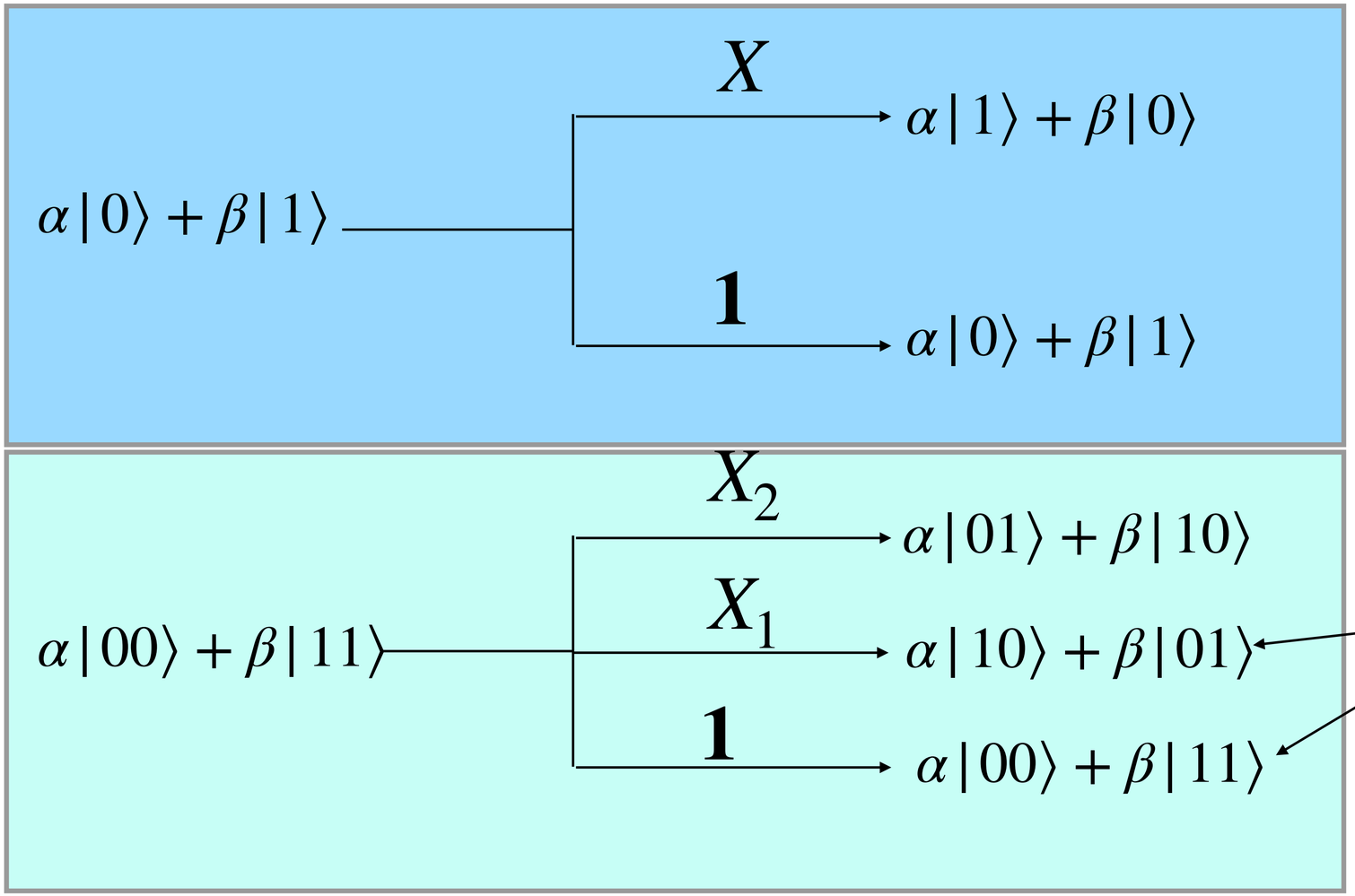
Question: Suppose we want to distinguish two orthonormal states $|\psi_1\rangle$ and $|\psi_2\rangle$. What is the operator that will do the job? Is it unique?

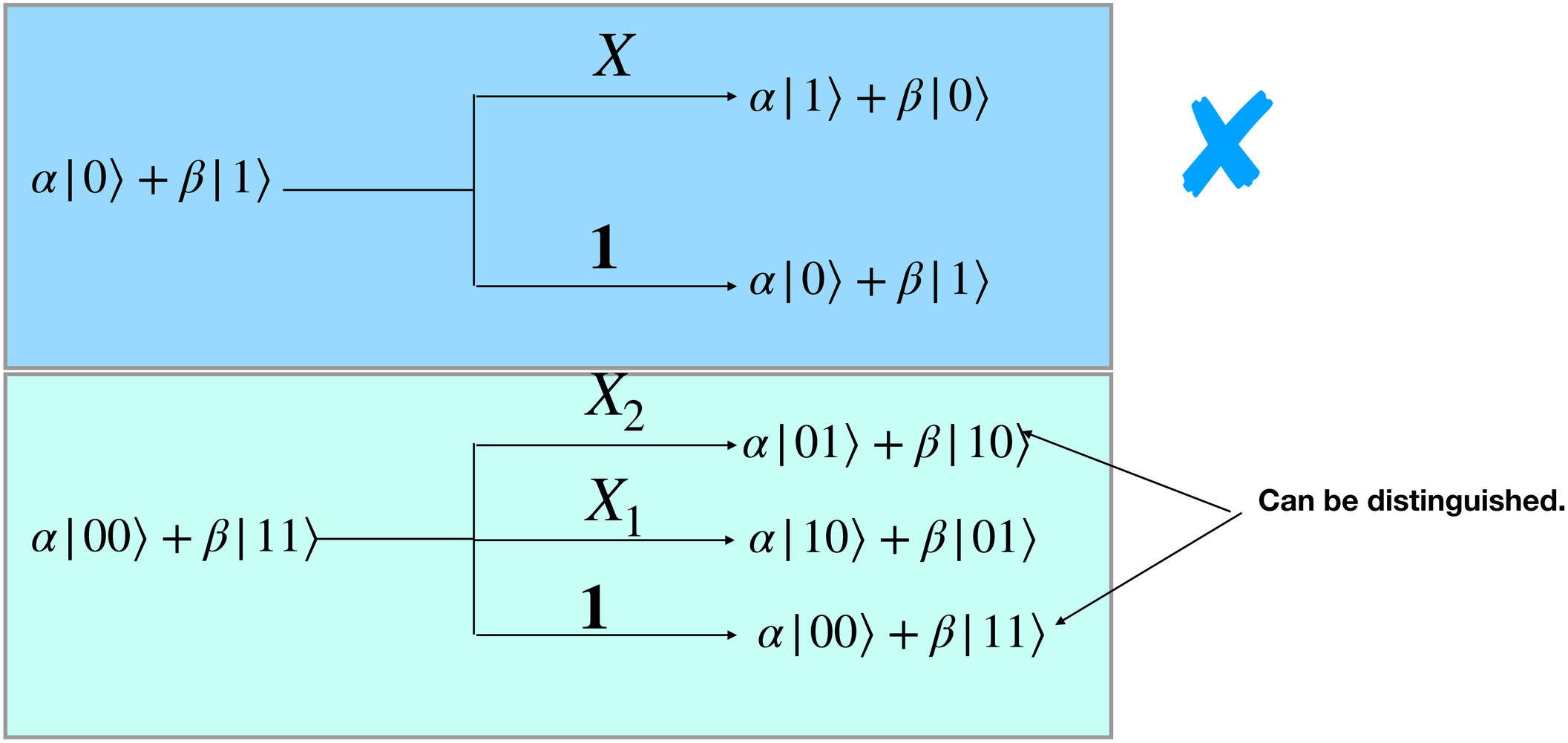
Orthogonal states can be unambiguously discriminated by measurement of a hermitian operator.

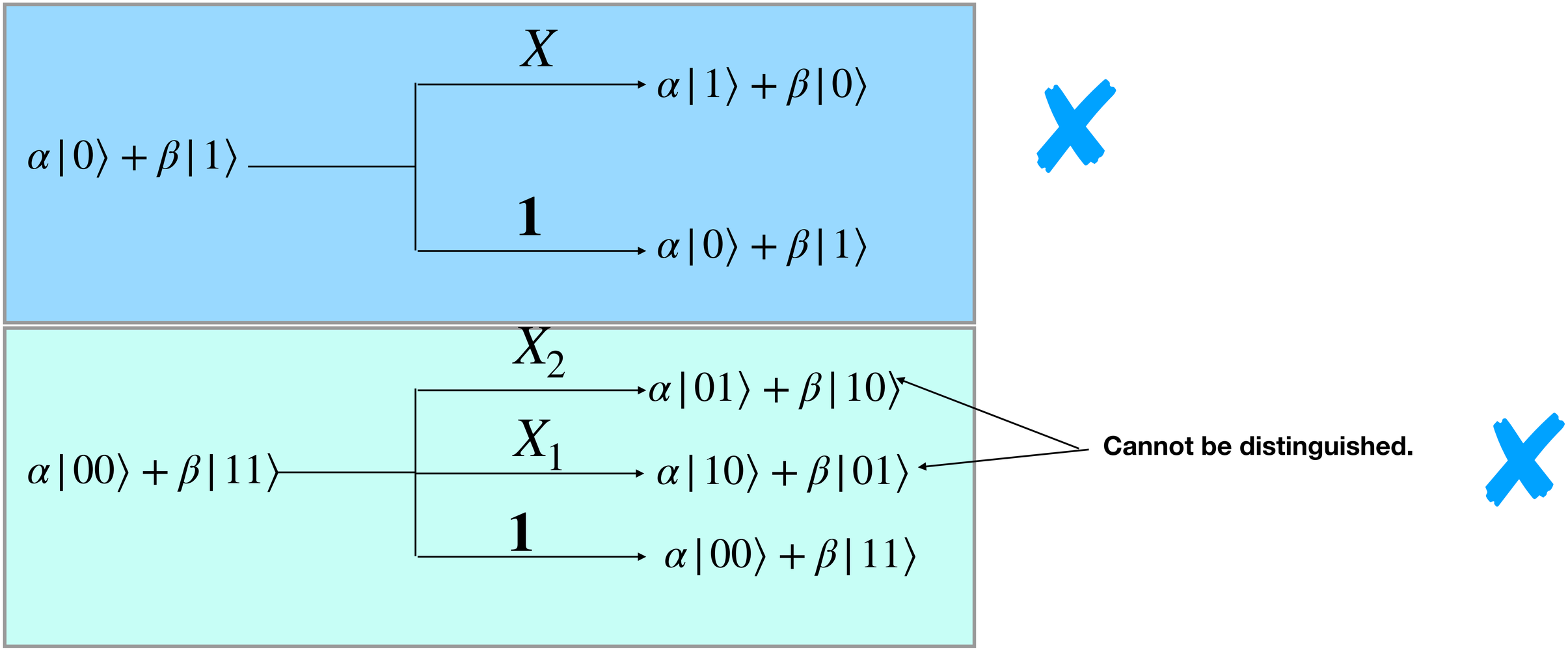
Question: Suppose we want to distinguish two orthonormal states $|\psi_1\rangle$ and $|\psi_2\rangle$. What is the operator that will do the job? Is it unique?

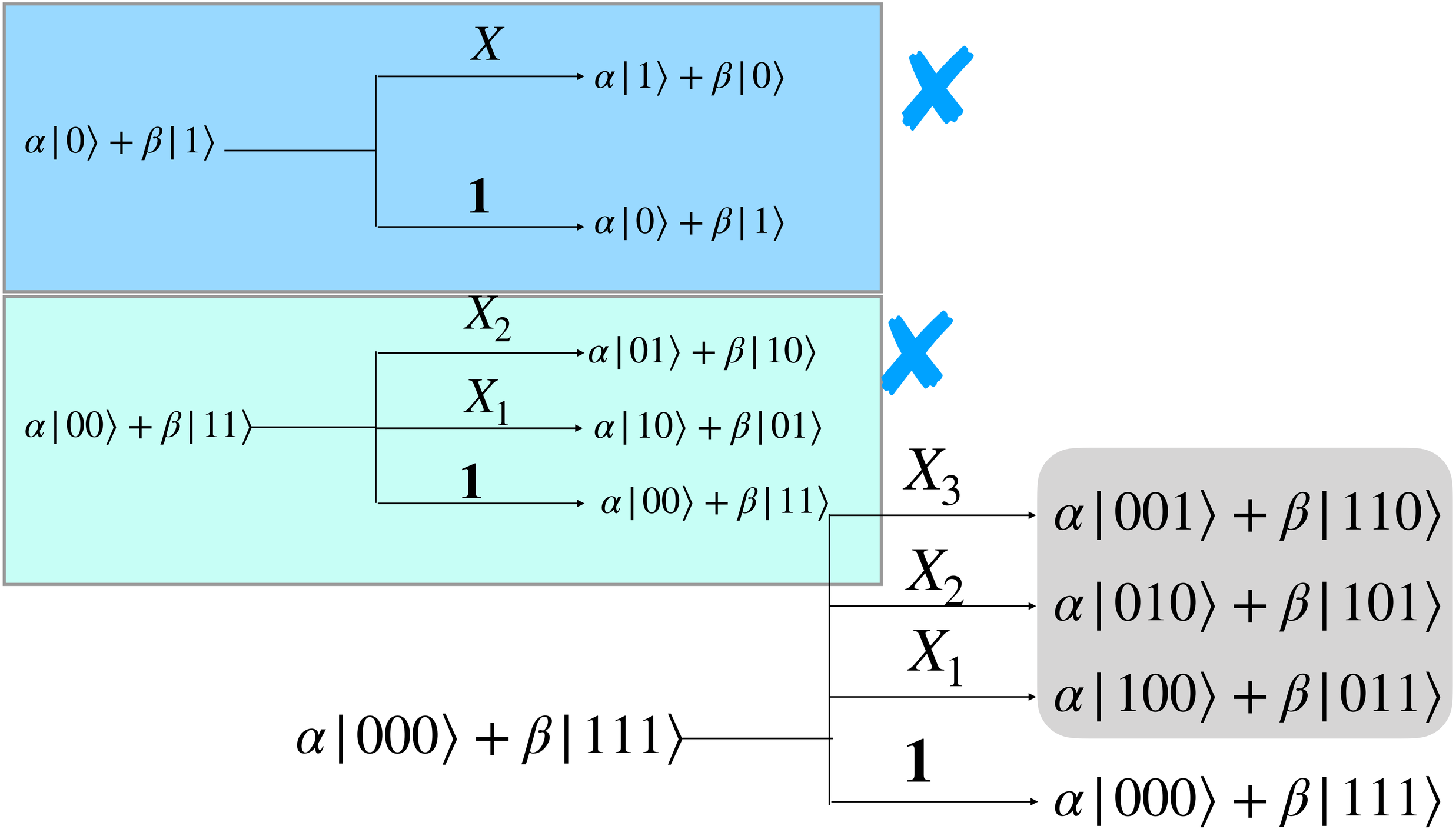
$$\lambda_1 |\psi_1\rangle\langle\psi_1| + \lambda_2 |\psi_2\rangle\langle\psi_2| ; \quad \lambda_1 \neq \lambda_2$$


X
$\alpha|1\rangle + \beta|0\rangle$
$\alpha|0\rangle + \beta|1\rangle$
$\mathbf{1}$
$\alpha|0\rangle + \beta|1\rangle$
X_2
$\alpha|01\rangle + \beta|10\rangle$
X_1
$\alpha|00\rangle + \beta|11\rangle$
$\alpha|10\rangle + \beta|01\rangle$
$\mathbf{1}$
$\alpha|00\rangle + \beta|11\rangle$

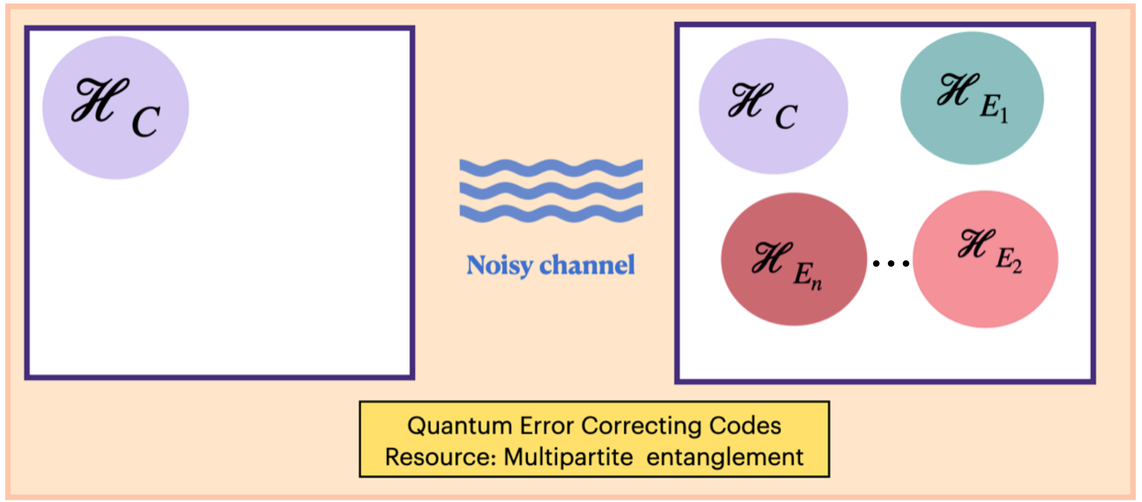

X
$\alpha|1\rangle + \beta|0\rangle$
$\alpha|0\rangle + \beta|1\rangle$
$\mathbf{1}$
$\alpha|0\rangle + \beta|1\rangle$
X_2
$\alpha|01\rangle + \beta|10\rangle$
X_1
$\alpha|00\rangle + \beta|11\rangle$
$\alpha|10\rangle + \beta|01\rangle$
$\mathbf{1}$
$\alpha|00\rangle + \beta|11\rangle$
Can be distinguished.


X
$\alpha|1\rangle + \beta|0\rangle$
$\alpha|0\rangle + \beta|1\rangle$
$\mathbf{1}$
$\alpha|0\rangle + \beta|1\rangle$
X_2
$\alpha|01\rangle + \beta|10\rangle$
X_1
$\alpha|10\rangle + \beta|01\rangle$
$\alpha|00\rangle + \beta|11\rangle$
$\mathbf{1}$
$\alpha|00\rangle + \beta|11\rangle$
Can be distinguished.


X
$\alpha|1\rangle + \beta|0\rangle$
$\alpha|0\rangle + \beta|1\rangle$
$\mathbf{1}$
$\alpha|0\rangle + \beta|1\rangle$
X_2
$\alpha|01\rangle + \beta|10\rangle$
X_1
$\alpha|10\rangle + \beta|01\rangle$
$\alpha|00\rangle + \beta|11\rangle$
$\mathbf{1}$
$\alpha|00\rangle + \beta|11\rangle$
Cannot be distinguished.

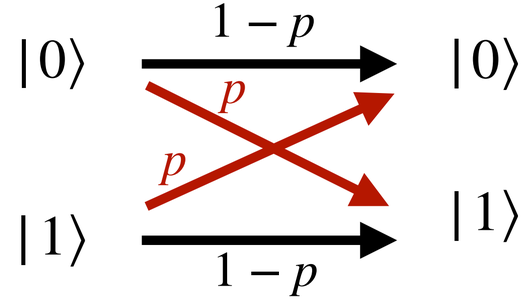

$\alpha|0\rangle + \beta|1\rangle$
X
$\alpha|1\rangle + \beta|0\rangle$
$\mathbf{1}$
$\alpha|0\rangle + \beta|1\rangle$
$\alpha|00\rangle + \beta|11\rangle$
X_2
$\alpha|01\rangle + \beta|10\rangle$
X_1
$\alpha|10\rangle + \beta|01\rangle$
$\mathbf{1}$
$\alpha|00\rangle + \beta|11\rangle$
$\alpha|000\rangle + \beta|111\rangle$
X_3
$\alpha|001\rangle + \beta|110\rangle$
X_2
$\alpha|010\rangle + \beta|101\rangle$
X_1
$\alpha|100\rangle + \beta|011\rangle$
$\mathbf{1}$
$\alpha|000\rangle + \beta|111\rangle$

Quantum error correcting codes: Bit flip channel



- **Single bit-flip** $\{\sqrt{p}, X_i\}$

$$X|0\rangle = |1\rangle$$
$$X|1\rangle = |0\rangle$$



$\mathcal{H}_C$: code space

$\mathcal{H}_{E_i}$: error space

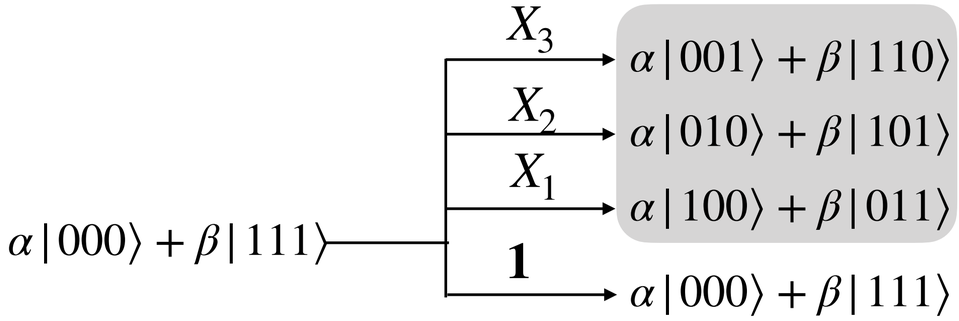
$$\mathcal{H}_C \perp \mathcal{H}_{E_1} \perp \mathcal{H}_{E_2} \perp \cdots \perp \mathcal{H}_{E_n} \Longrightarrow$$

Resource state $\alpha|000\rangle + \beta|111\rangle$

WHY THREE?

Error on each qubits → Two-dim subspace

No error→Two dim subspace



WHY THREE?

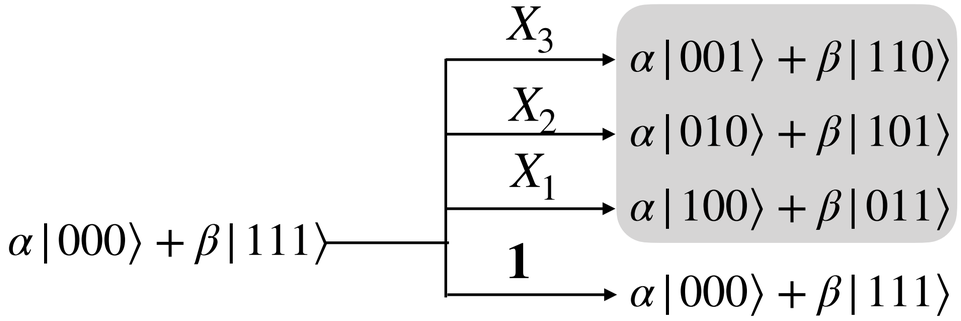
Error on each qubits → Two-dim subspace

No error→Two dim subspace

$$2(n+1)$$

Number of qubits

Uncorrupted case



WHY THREE?

Error on each qubits → Two-dim subspace

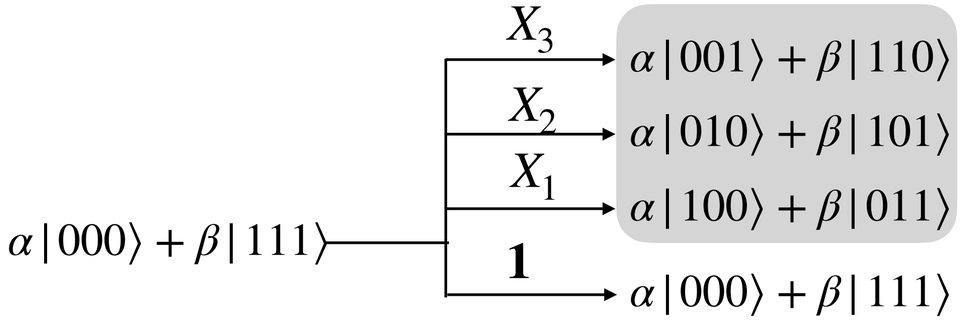
No error→Two dim subspace

$$2(n+1)$$

Number of qubits

Uncorrupted case

Each of them should belong to different two dimensional subspaces



WHY THREE?

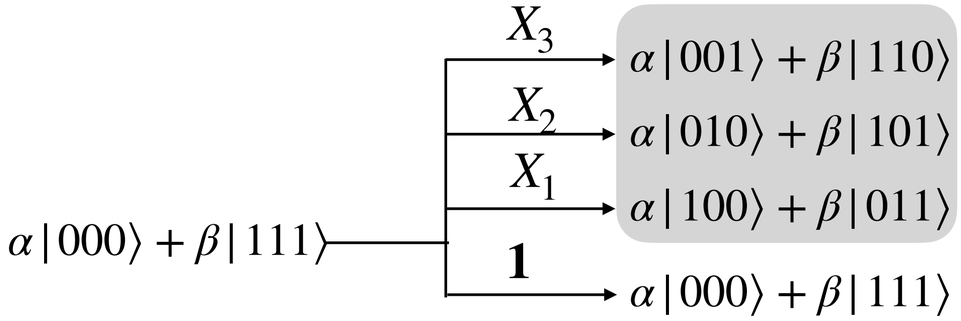
$$2^n \geq 2(n+1)$$

Dimension of Hilbert space to which the logical state belongs.

Number of qubits

Uncorrupted case

Each of them should belong to different two dimensional subspaces



How to identify which error has occurred?

How to identify which error has occurred?

Measure

How to identify which error has occurred?

Measure

But Born’s rule?

Way out: Measure the Error, Not the Data

Quantum error correcting codes: Bit flip channel

Resource state $\alpha|000\rangle + \beta|111\rangle$

$$\xrightarrow{X_1} \alpha|100\rangle + \beta|011\rangle$$

$$\xrightarrow{X_2} \alpha|010\rangle + \beta|101\rangle$$

$$\xrightarrow{X_3} \alpha|001\rangle + \beta|110\rangle$$

Z_1Z_2	Z_2Z_3
$+1$	$+1$
-1	$+1$
-1	-1
$+1$	-1

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$Z_1 Z_2 \equiv Z_1 \otimes Z_2 \otimes \mathbf{1}$$

$$= (|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes (|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|)$$

$$= (|00\rangle\langle 00| - |01\rangle\langle 01| - |10\rangle\langle 10| + |11\rangle\langle 11|) \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|)$$

$$= (|000\rangle\langle 000| - |010\rangle\langle 010| - |100\rangle\langle 100| + |110\rangle\langle 110|) +$$

$$(|001\rangle\langle 001| - |011\rangle\langle 011| - |101\rangle\langle 101| + |111\rangle\langle 111|)$$

Quantum error correcting codes: Bit flip channel

Resource state $\alpha|000\rangle + \beta|111\rangle$

$$\xrightarrow{X_1} \alpha|100\rangle + \beta|011\rangle$$

$$\xrightarrow{X_2} \alpha|010\rangle + \beta|101\rangle$$

$$\xrightarrow{X_3} \alpha|001\rangle + \beta|110\rangle$$

QUESTION: VERIFY IT!!!

Z_1Z_2	Z_2Z_3
$+1$	$+1$
-1	$+1$
-1	-1
$+1$	-1

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Quantum error correcting codes: Bit flip channel

Resource state $\alpha|000\rangle + \beta|111\rangle$

$$\xrightarrow{X_1} \alpha|100\rangle + \beta|011\rangle$$

$$\xrightarrow{X_2} \alpha|010\rangle + \beta|101\rangle$$

$$\xrightarrow{X_3} \alpha|001\rangle + \beta|110\rangle$$

Parity check between the first two

Z_1Z_2	Z_2Z_3
$+1$	$+1$
-1	$+1$
-1	-1
$+1$	-1

Parity check between the last two

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Quantum error correcting codes: Bit flip channel

Resource state $\alpha|000\rangle + \beta|111\rangle$

$$\alpha|000\rangle + \beta|111\rangle \xrightarrow{X_1} \alpha|100\rangle + \beta|011\rangle$$
$$\alpha|000\rangle + \beta|111\rangle \xrightarrow{X_2} \alpha|010\rangle + \beta|101\rangle$$
$$\alpha|000\rangle + \beta|111\rangle \xrightarrow{X_3} \alpha|001\rangle + \beta|110\rangle$$

Z_1Z_2	Z_2Z_3	How to correct?
$+1$	$+1$	**1**
-1	$+1$	
-1	-1	
$+1$	-1	

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Quantum error correcting codes: Bit flip channel

Resource state $\alpha|000\rangle + \beta|111\rangle$

$$\alpha|000\rangle + \beta|111\rangle \xrightarrow{X_1} \begin{cases} \alpha|100\rangle + \beta|011\rangle \xrightarrow{X_1} \alpha|000\rangle + \beta|111\rangle \\ \alpha|010\rangle + \beta|101\rangle \\ \alpha|001\rangle + \beta|110\rangle \end{cases}$$

Z_1Z_2	Z_2Z_3	How to correct?
$+1$	$+1$	$\mathbf{1}$
-1	$+1$	X_1
-1	-1	
$+1$	-1	

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Quantum error correcting codes: Bit flip channel

Resource state $\alpha|000\rangle + \beta|111\rangle$

$$\alpha|000\rangle + \beta|111\rangle \xrightarrow{X_1} \begin{cases} \alpha|100\rangle + \beta|011\rangle \xrightarrow{X_1} \alpha|000\rangle + \beta|111\rangle \\ \alpha|010\rangle + \beta|101\rangle \xrightarrow{X_2} \alpha|000\rangle + \beta|111\rangle \\ \alpha|001\rangle + \beta|110\rangle \end{cases}$$

Z_1Z_2	Z_2Z_3	How to correct?
$+1$	$+1$	$\mathbf{1}$
-1	$+1$	X_1
-1	-1	X_2
$+1$	-1	

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Quantum error correcting codes: Bit flip channel

Resource state $\alpha|000\rangle + \beta|111\rangle$

$$\alpha|000\rangle + \beta|111\rangle \xrightarrow{X_1} \alpha|100\rangle + \beta|011\rangle \xrightarrow{X_1} \alpha|000\rangle + \beta|111\rangle$$

$$\alpha|000\rangle + \beta|111\rangle \xrightarrow{X_2} \alpha|010\rangle + \beta|101\rangle \xrightarrow{X_2} \alpha|000\rangle + \beta|111\rangle$$

$$\alpha|000\rangle + \beta|111\rangle \xrightarrow{X_3} \alpha|001\rangle + \beta|110\rangle \xrightarrow{X_3} \alpha|000\rangle + \beta|111\rangle$$

Z_1Z_2	Z_2Z_3	How to correct?
$+1$	$+1$	$\mathbf{1}$
-1	$+1$	X_1
-1	-1	X_2
$+1$	-1	X_3

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Do we get the correct state in the end in each iteration?

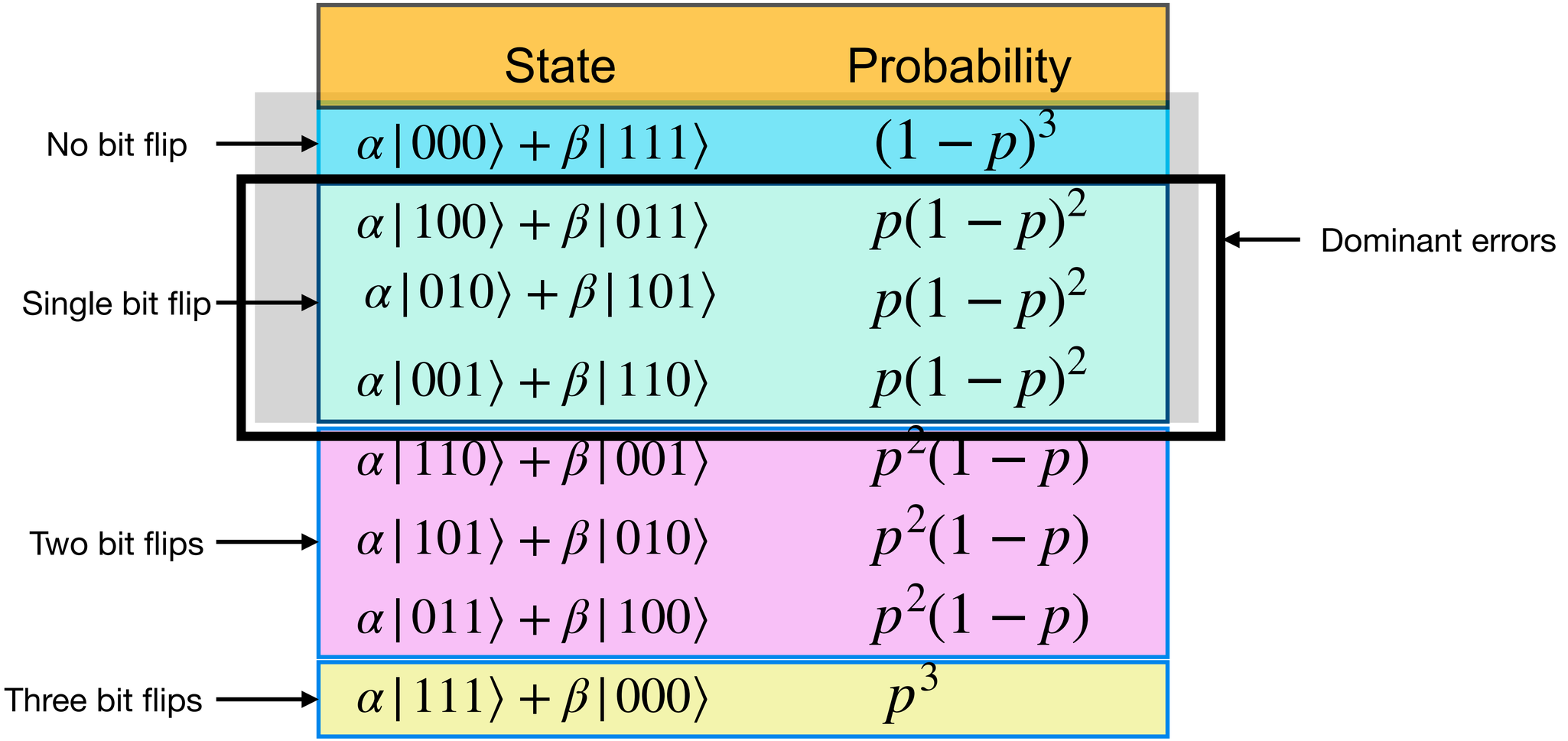
After a bit flip channel →8 possible results

p: probability of single bit-flip

	State	Probability
No bit flip	$\alpha\|000\rangle + \beta\|111\rangle$	$(1-p)^3$
Single bit flip	$\alpha\|100\rangle + \beta\|011\rangle$	$p(1-p)^2$
	$\alpha\|010\rangle + \beta\|101\rangle$	$p(1-p)^2$
	$\alpha\|001\rangle + \beta\|110\rangle$	$p(1-p)^2$
Two bit flips	$\alpha\|110\rangle + \beta\|001\rangle$	$p^2(1-p)$
	$\alpha\|101\rangle + \beta\|010\rangle$	$p^2(1-p)$
	$\alpha\|011\rangle + \beta\|100\rangle$	$p^2(1-p)$
Three bit flips	$\alpha\|111\rangle + \beta\|000\rangle$	p^3

Then why only single qubit error considered?

After a bit flip channel →8 possible results



$p=0.1$

Probability of a single bit flip=$3p(1-p)^2\approx 0.24$

Probability of two bit flips=$3p^2(1-p)\approx 0.027$

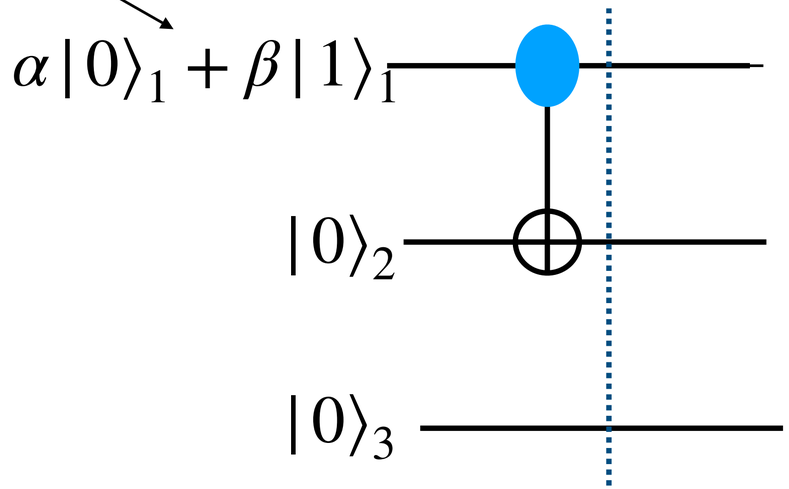
Probability of three bit flips=$p^3=0.001$

How to realise these tasks?

Encoding a logical qubit in three physical qubits

$$(\alpha|0\rangle + \beta|1\rangle)|00\rangle \xrightarrow{U} \alpha|000\rangle + \beta|111\rangle$$

Encoder

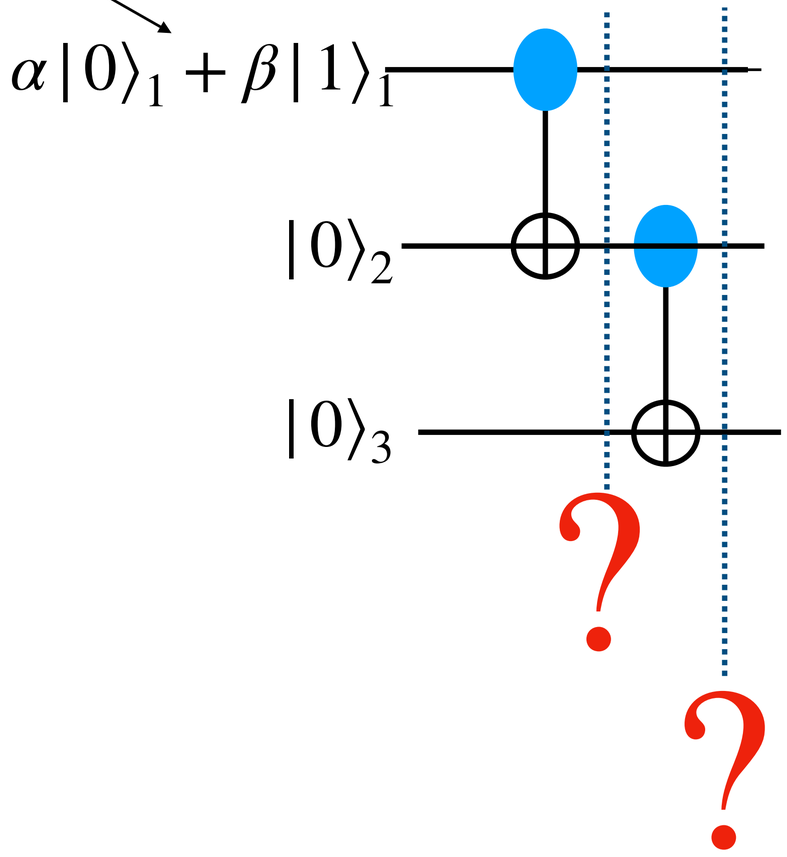


$$(\alpha|0\rangle_1 + \beta|1\rangle_1)|0\rangle_2|0\rangle_3$$

Encoding a logical qubit in three physical qubits

$$(\alpha|0\rangle + \beta|1\rangle)|00\rangle \xrightarrow{U} \alpha|000\rangle + \beta|111\rangle$$

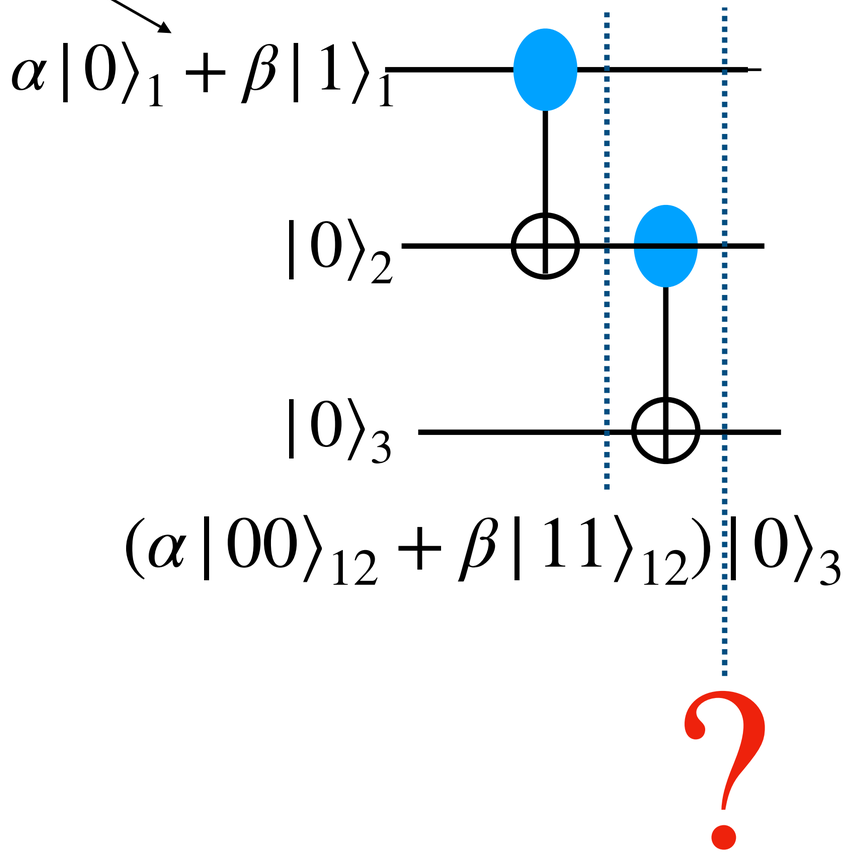
Encoder



Encoding a logical qubit in three physical qubits

$$(\alpha|0\rangle + \beta|1\rangle)|00\rangle \xrightarrow{U} \alpha|000\rangle + \beta|111\rangle$$

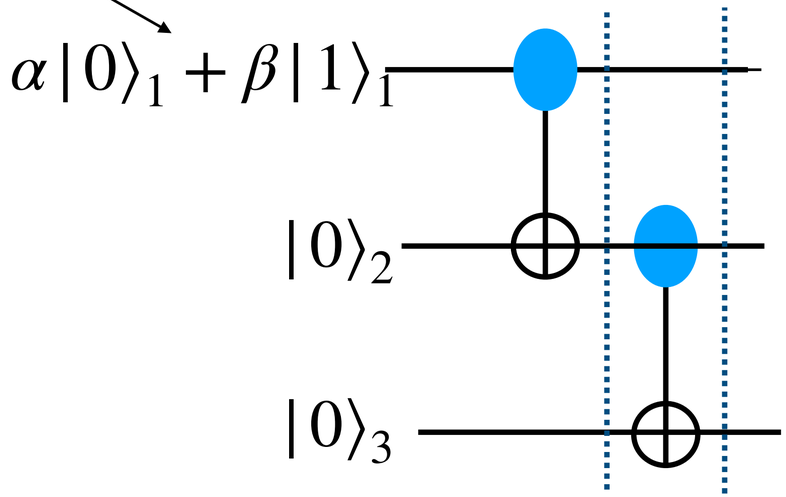
Encoder



Encoding a logical qubit in three physical qubits

$$(\alpha|0\rangle + \beta|1\rangle)|00\rangle \xrightarrow{U} \alpha|000\rangle + \beta|111\rangle$$

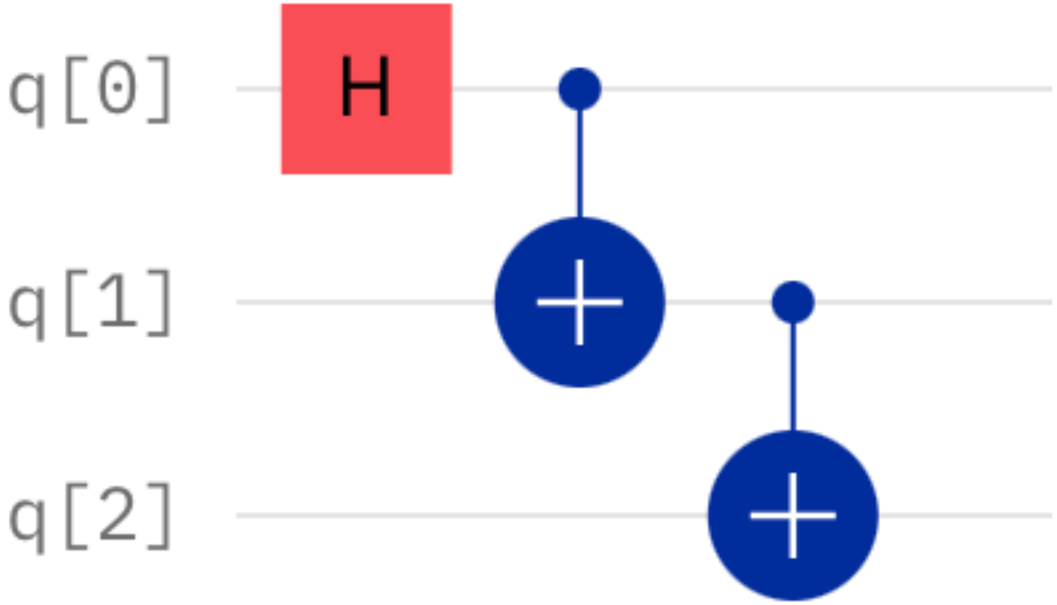
Encoder

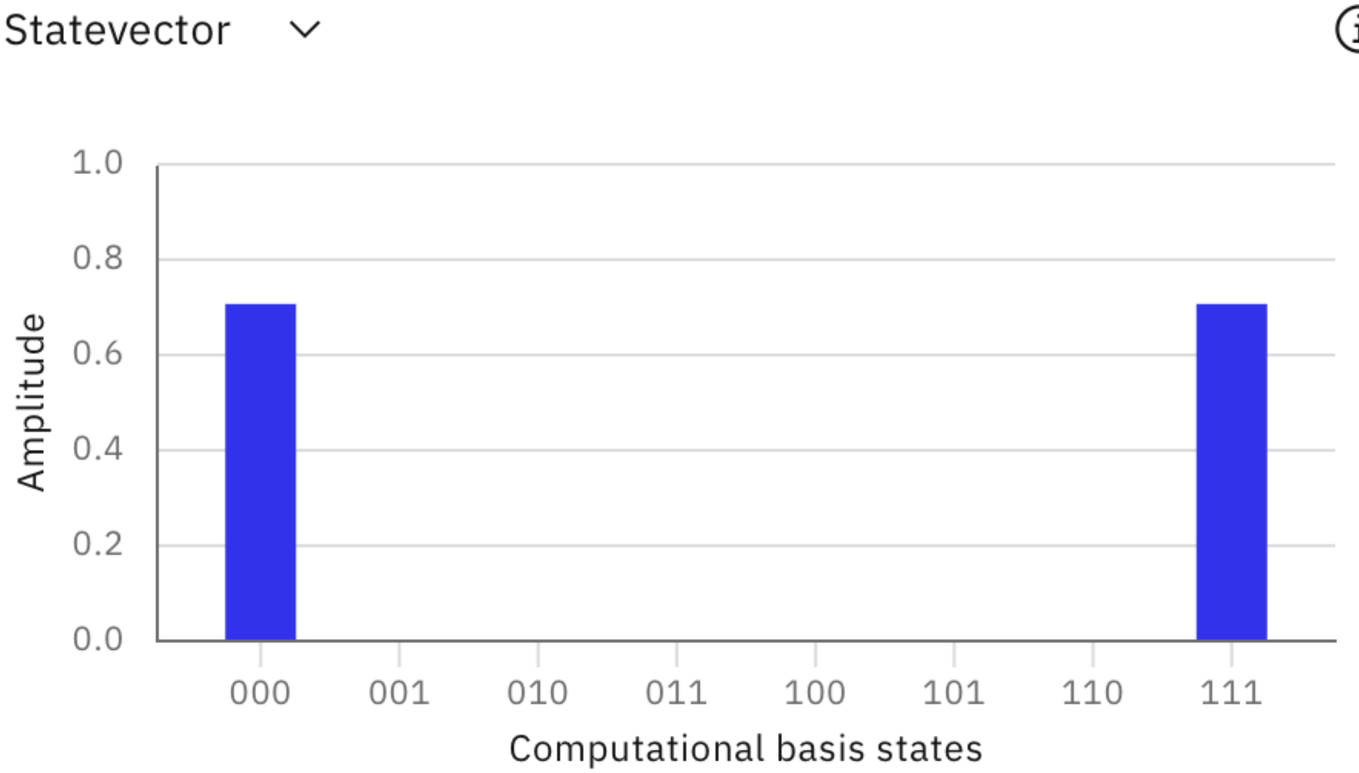


$$(\alpha|00\rangle_{12} + \beta|11\rangle_{12})|0\rangle_3$$

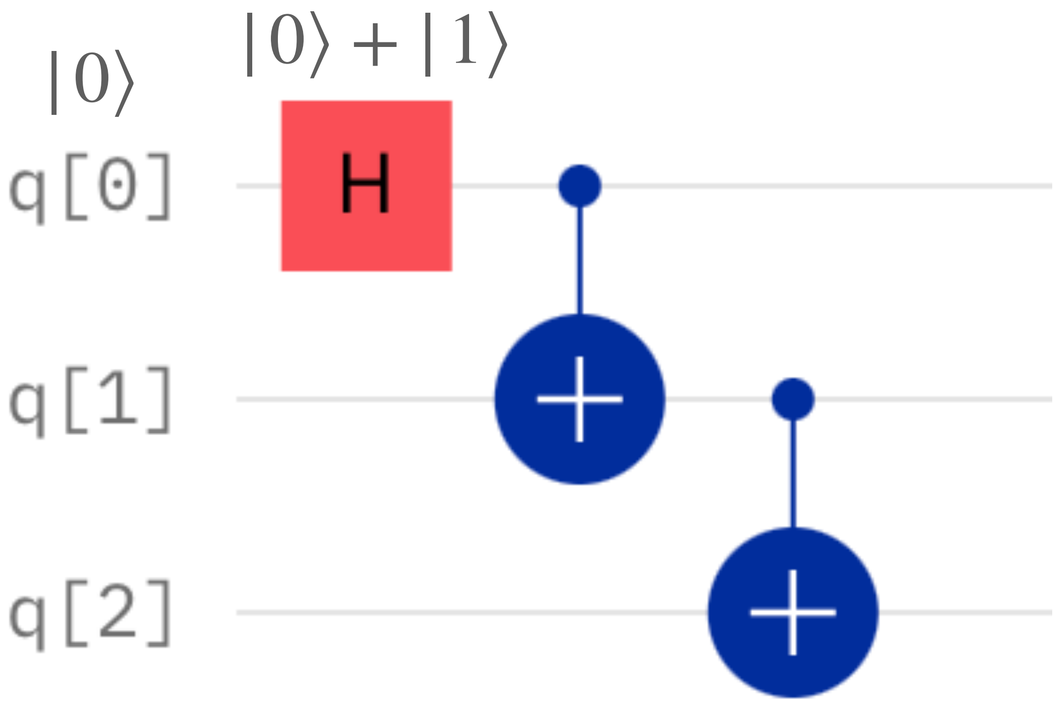
$$\alpha|000\rangle_{123} + \beta|111\rangle_{123}$$

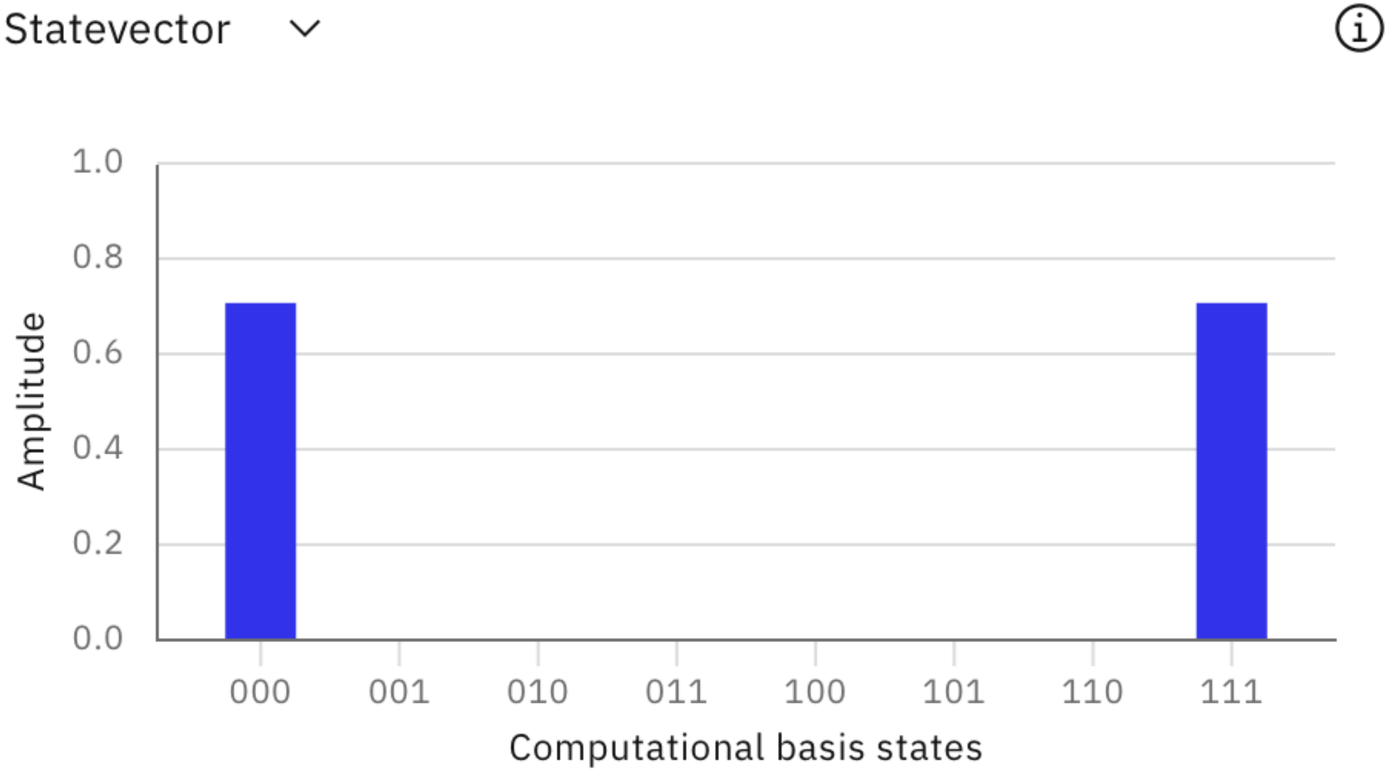
On Q-composer
Generation of a logical state





On Q-composer
Generation of a logical state

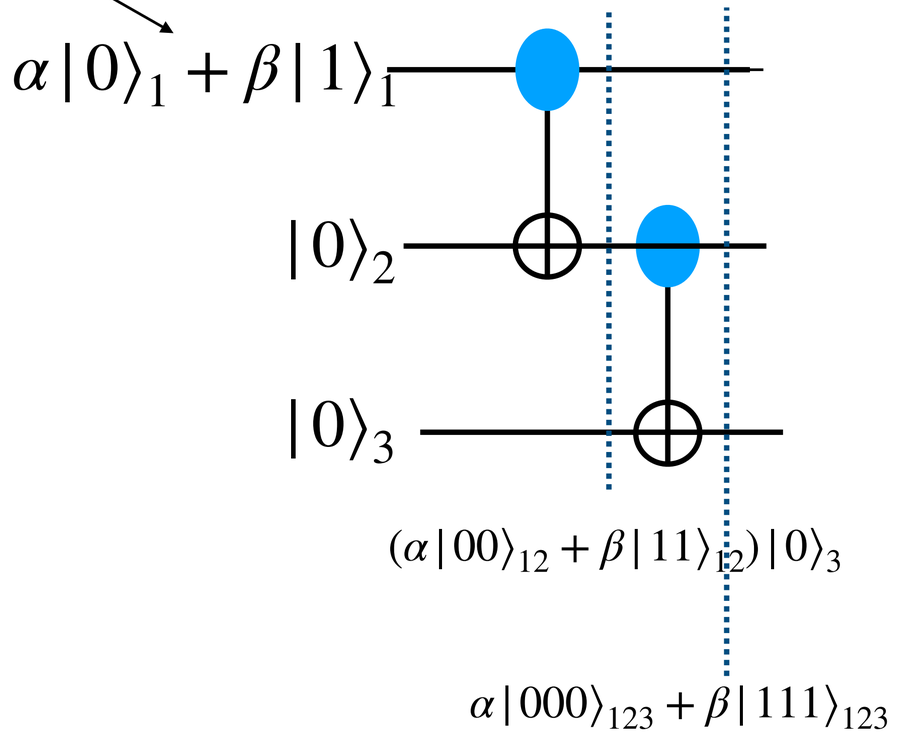




Encoding a logical qubit in three physical qubits

$$(\alpha|0\rangle + \beta|1\rangle)|00\rangle \xrightarrow{U} \alpha|000\rangle + \beta|111\rangle$$

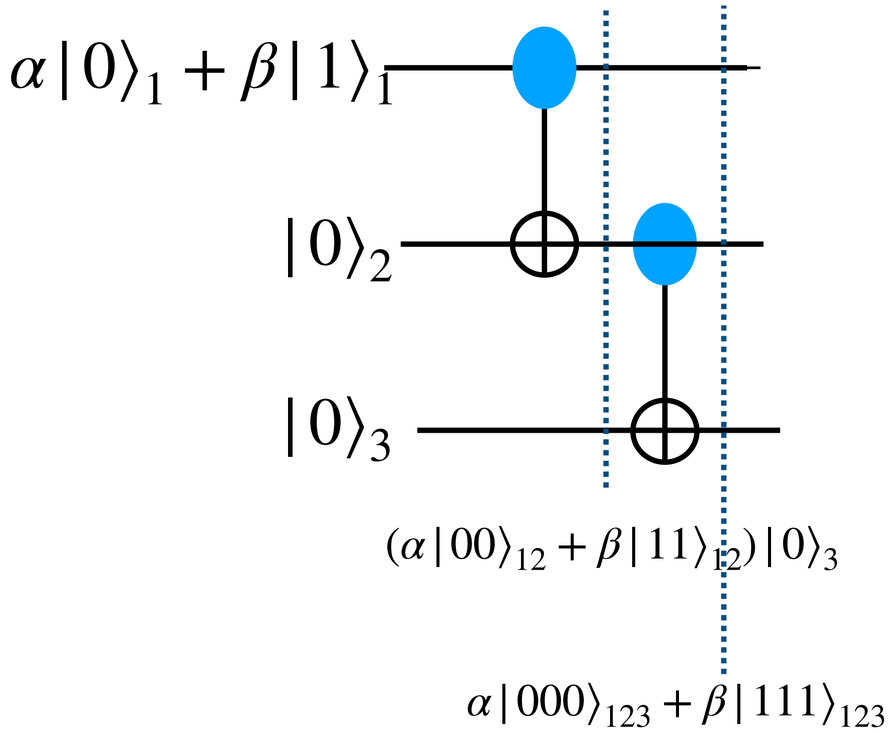
Encoder



Example: Bit flip error (X) on 2nd qubit:

$$\alpha|010\rangle + \beta|101\rangle$$

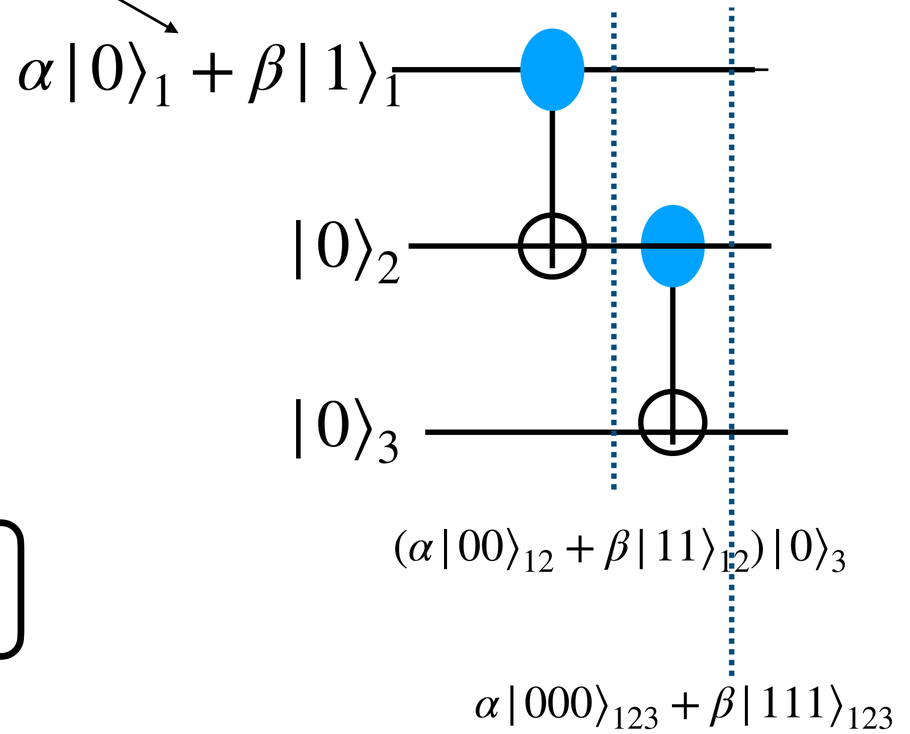
2nd qubit is now different from 1st and 3rd.


$\alpha|0\rangle_1 + \beta|1\rangle_1$
$|0\rangle_2$
$|0\rangle_3$
$(\alpha|00\rangle_{12} + \beta|11\rangle_{12})|0\rangle_3$
$\alpha|000\rangle_{123} + \beta|111\rangle_{123}$

Encoding a logical qubit in three physical qubits

$$(\alpha|0\rangle + \beta|1\rangle)|00\rangle \xrightarrow{U} \alpha|000\rangle + \beta|111\rangle$$

Encoder



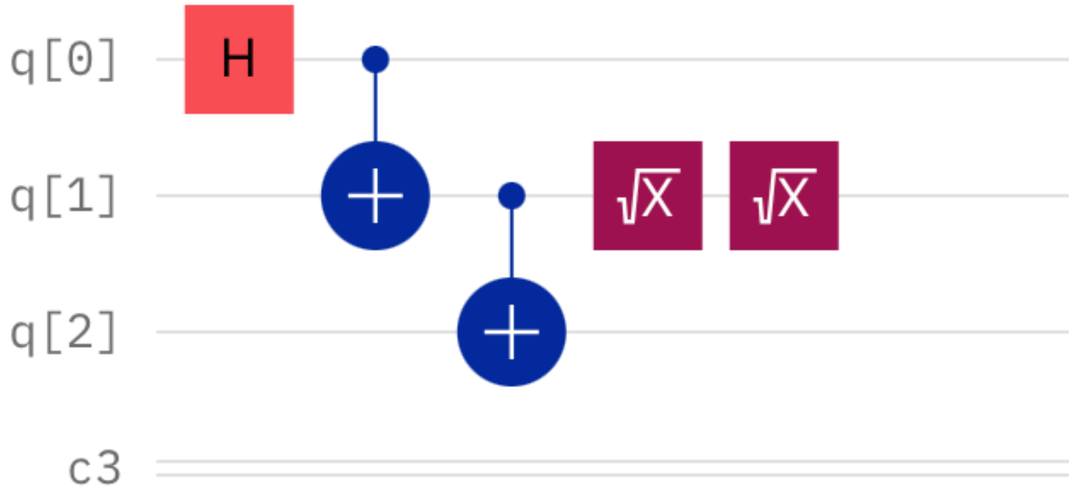
Example: Bit flip error (X) on 2nd qubit:

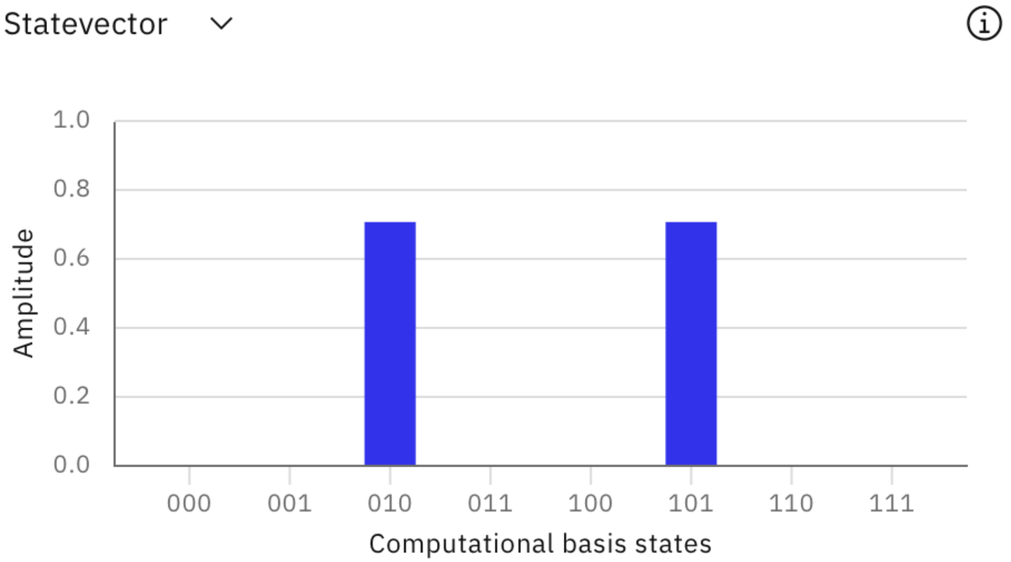
$$\alpha|010\rangle + \beta|101\rangle$$

2nd qubit is now different from 1st and 3rd.

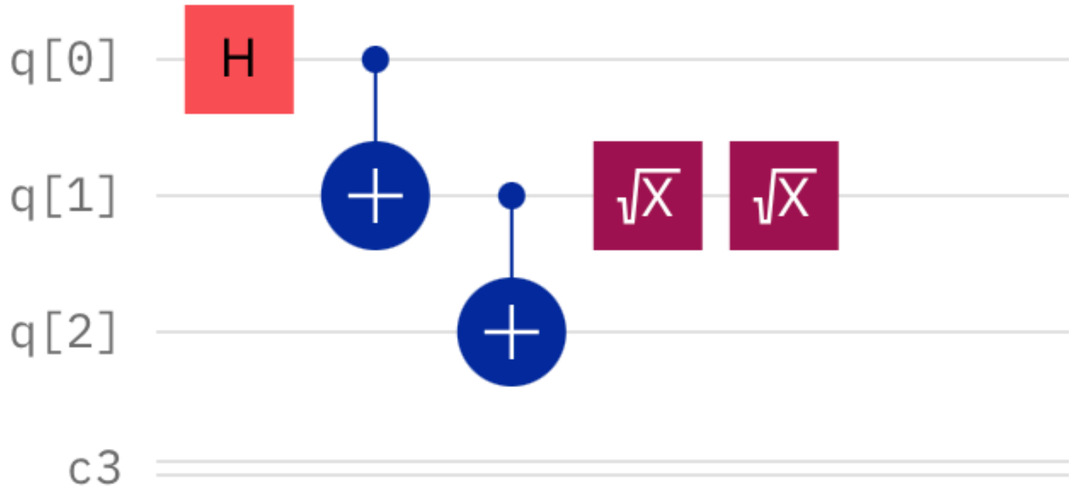
We wish to measure that it is different without finding its actual value.

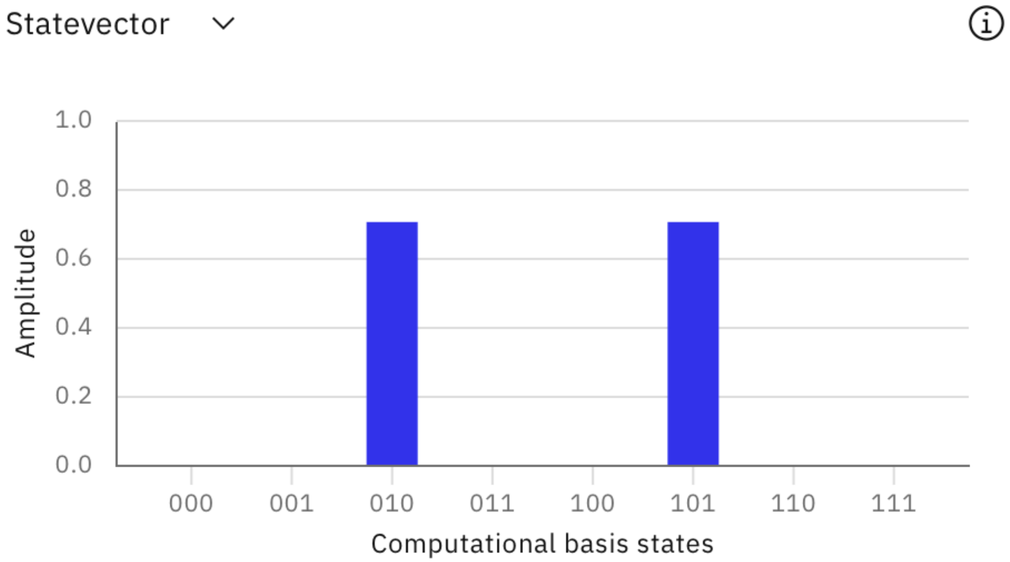
On Q-composer
Bit flip on the second qubit

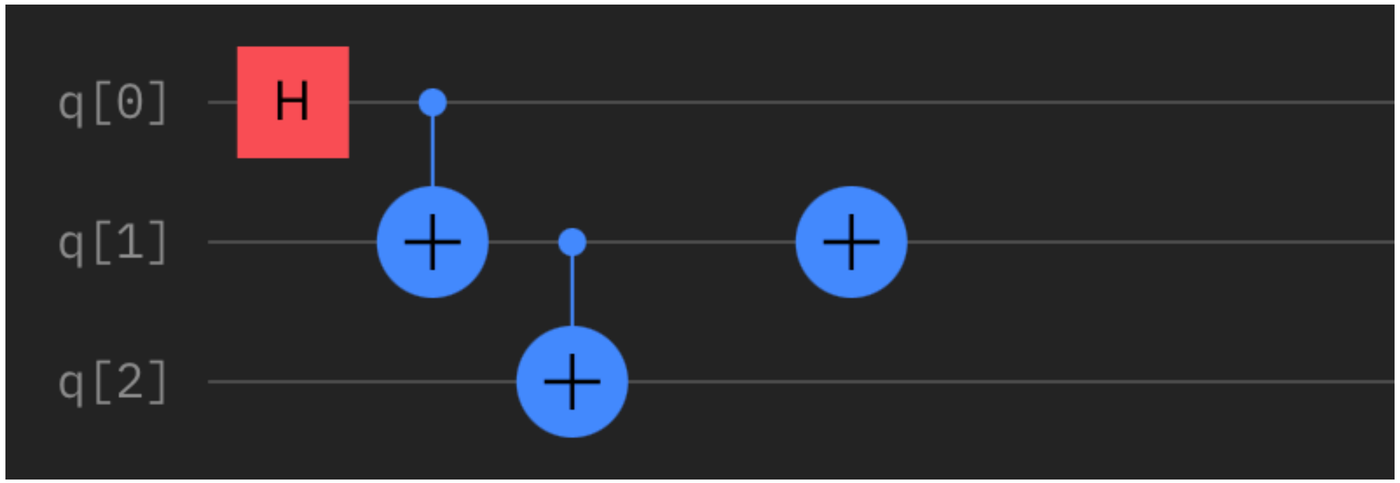


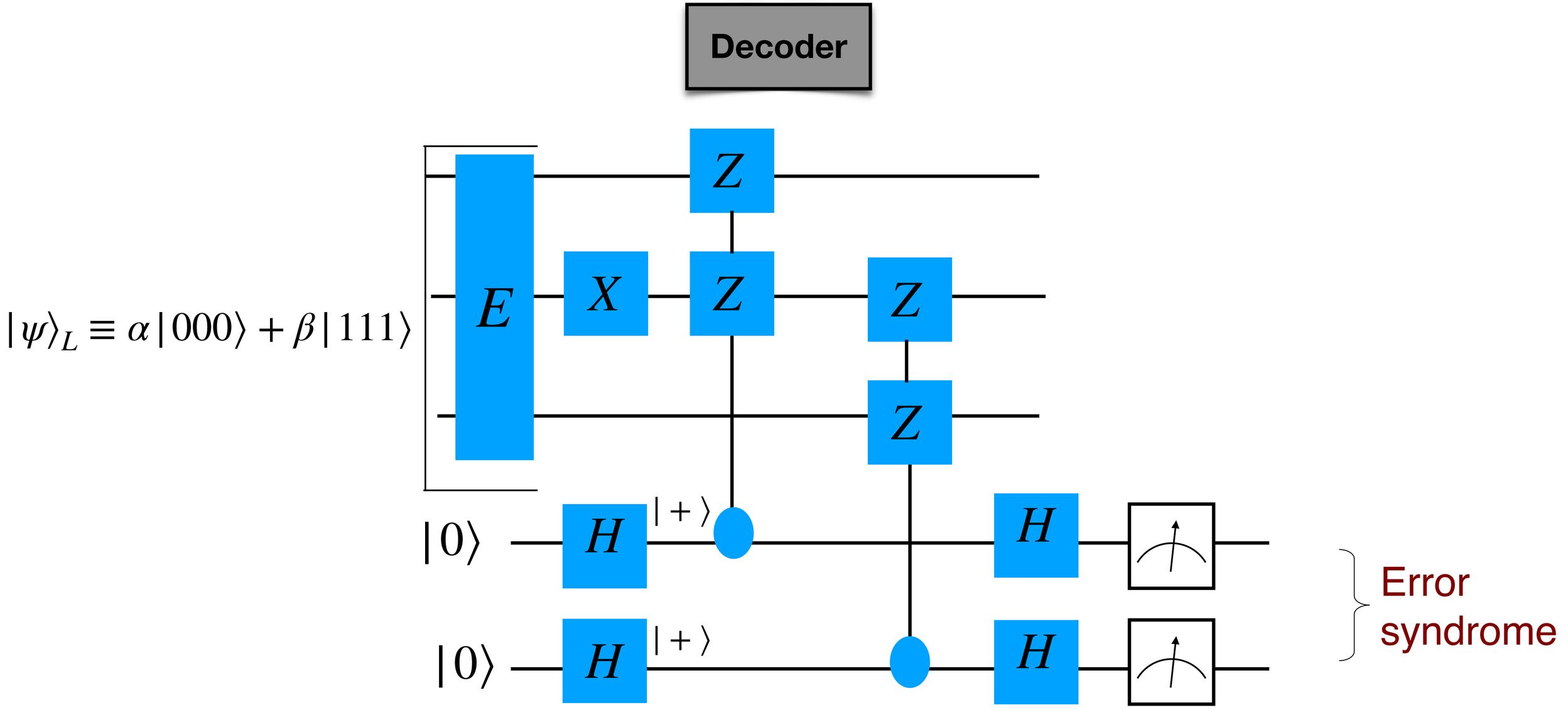


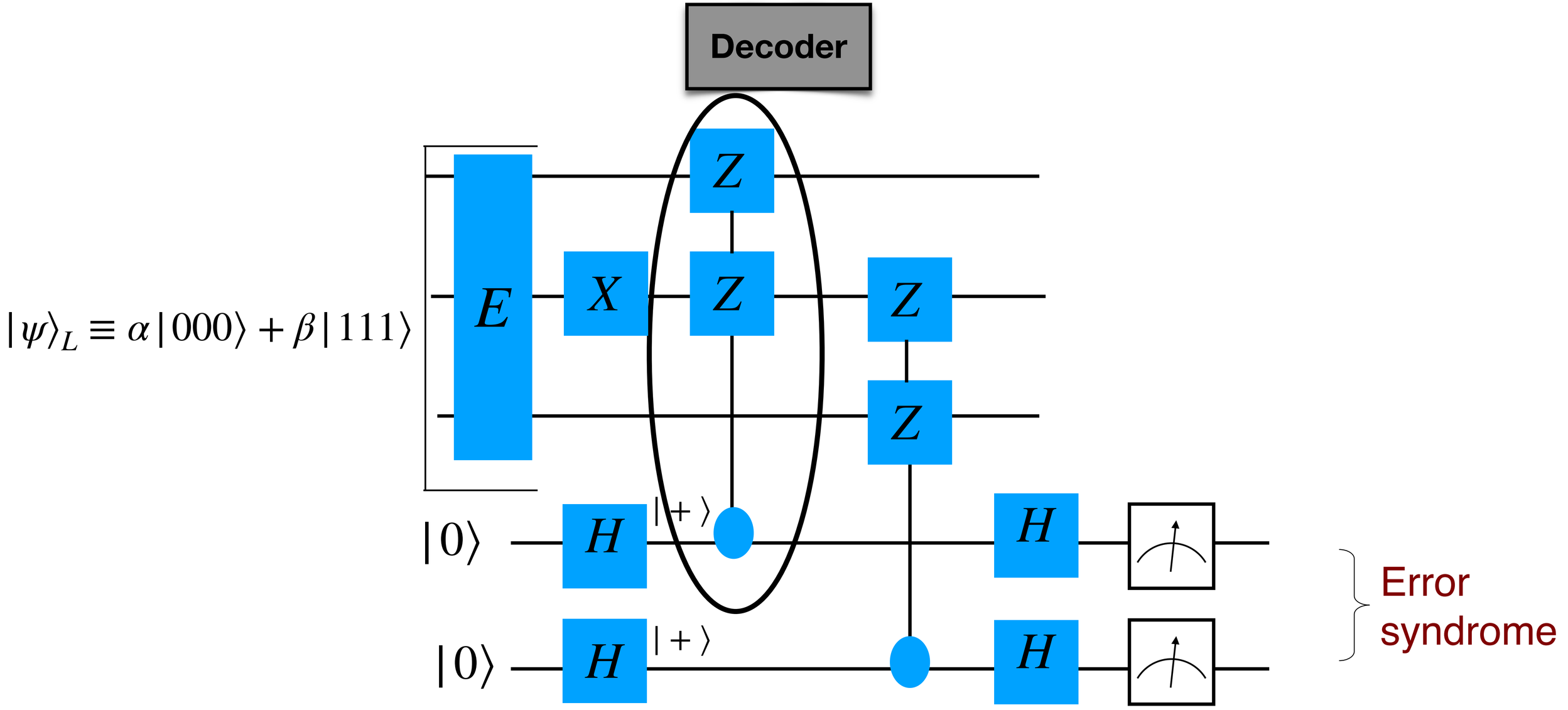
On Q-composer
Bit flip on the second qubit

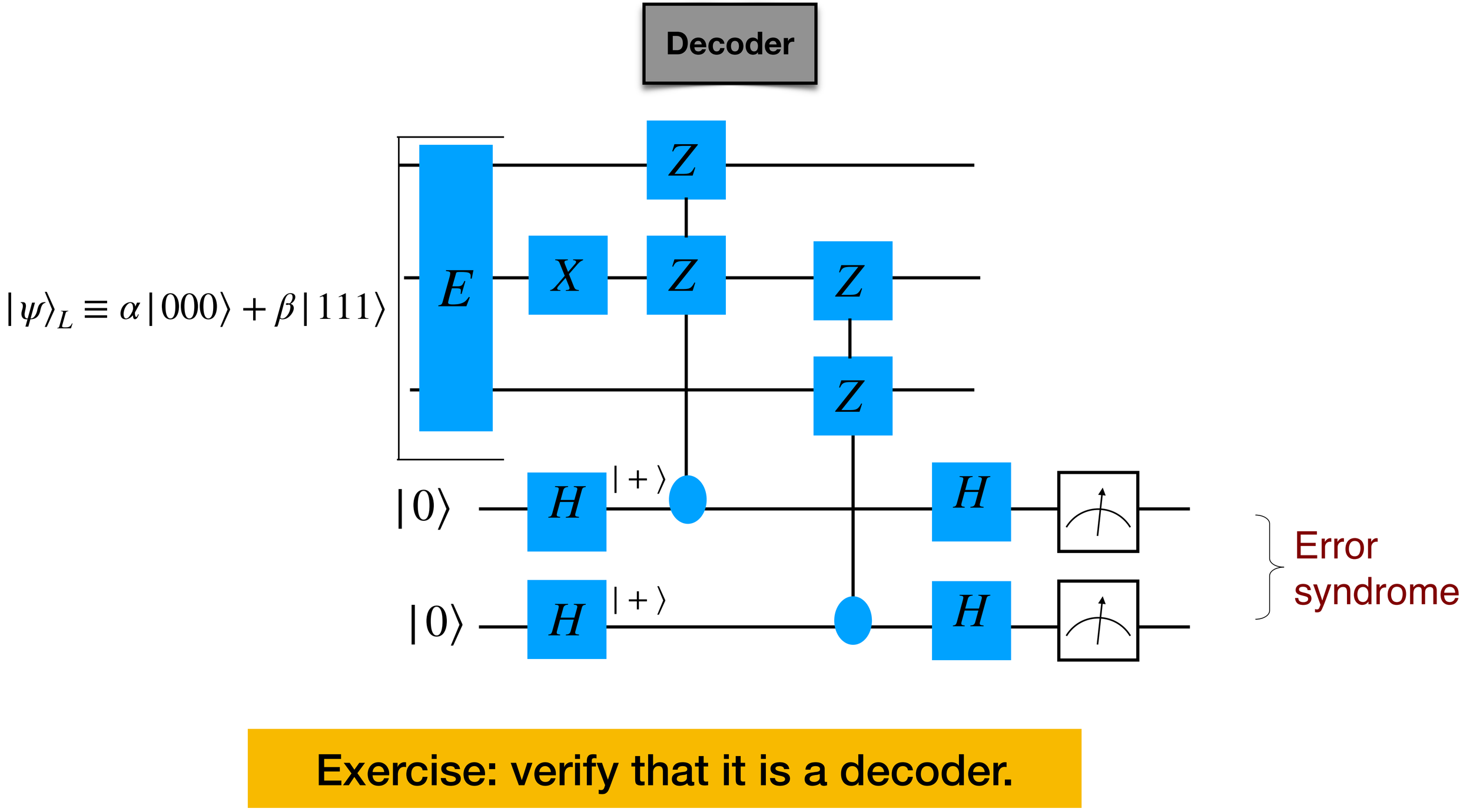







Decoder
$|\psi\rangle_L \equiv \alpha|000\rangle + \beta|111\rangle$
E
X
Z
Z
Z
Z
$|0\rangle$
H
$|+\rangle$
H
$|0\rangle$
H
$|+\rangle$
H
Error syndrome


Decoder
$|\psi\rangle_L \equiv \alpha|000\rangle + \beta|111\rangle$
E
X
Z
Z
Z
Z
$|0\rangle$
H
$|+\rangle$
H
$|0\rangle$
H
$|+\rangle$
H
Error syndrome



Exercise: verify that it is a decoder.

On Q-composer
Decoder

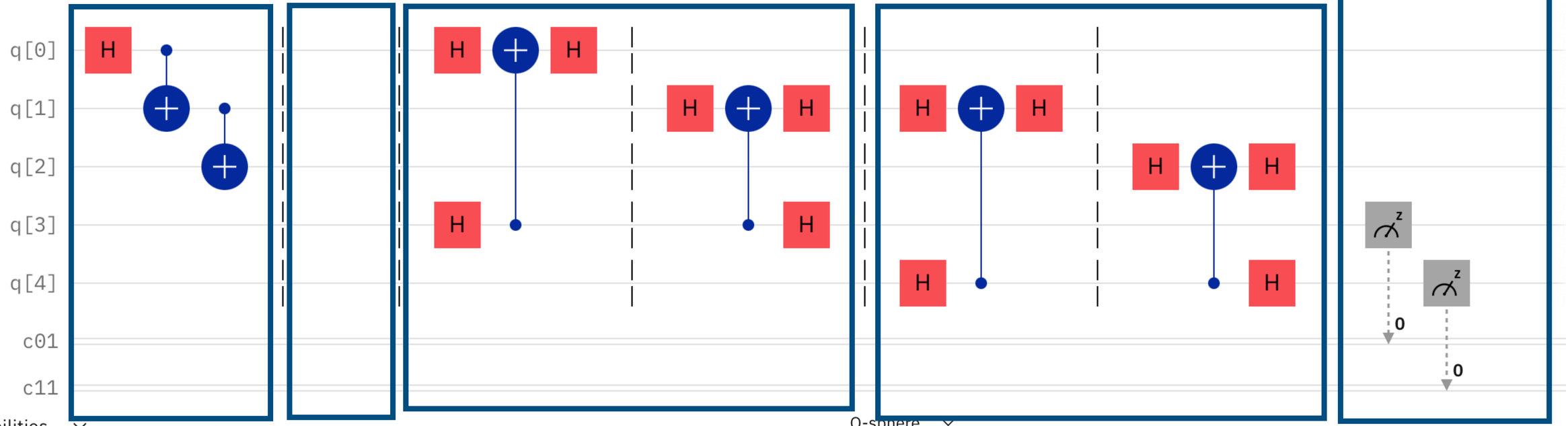
Encoder

No error

Z_1Z_2

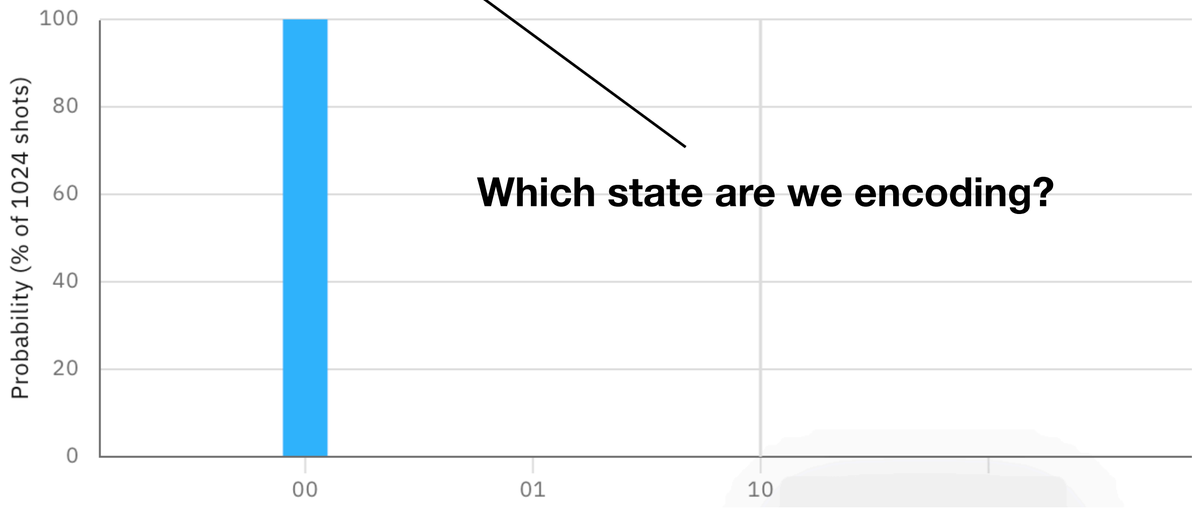
Z_2Z_3

Measurement

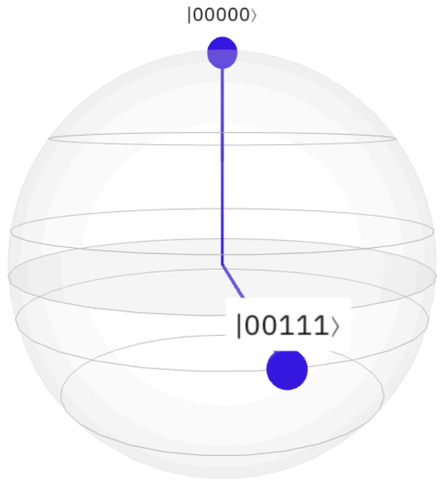


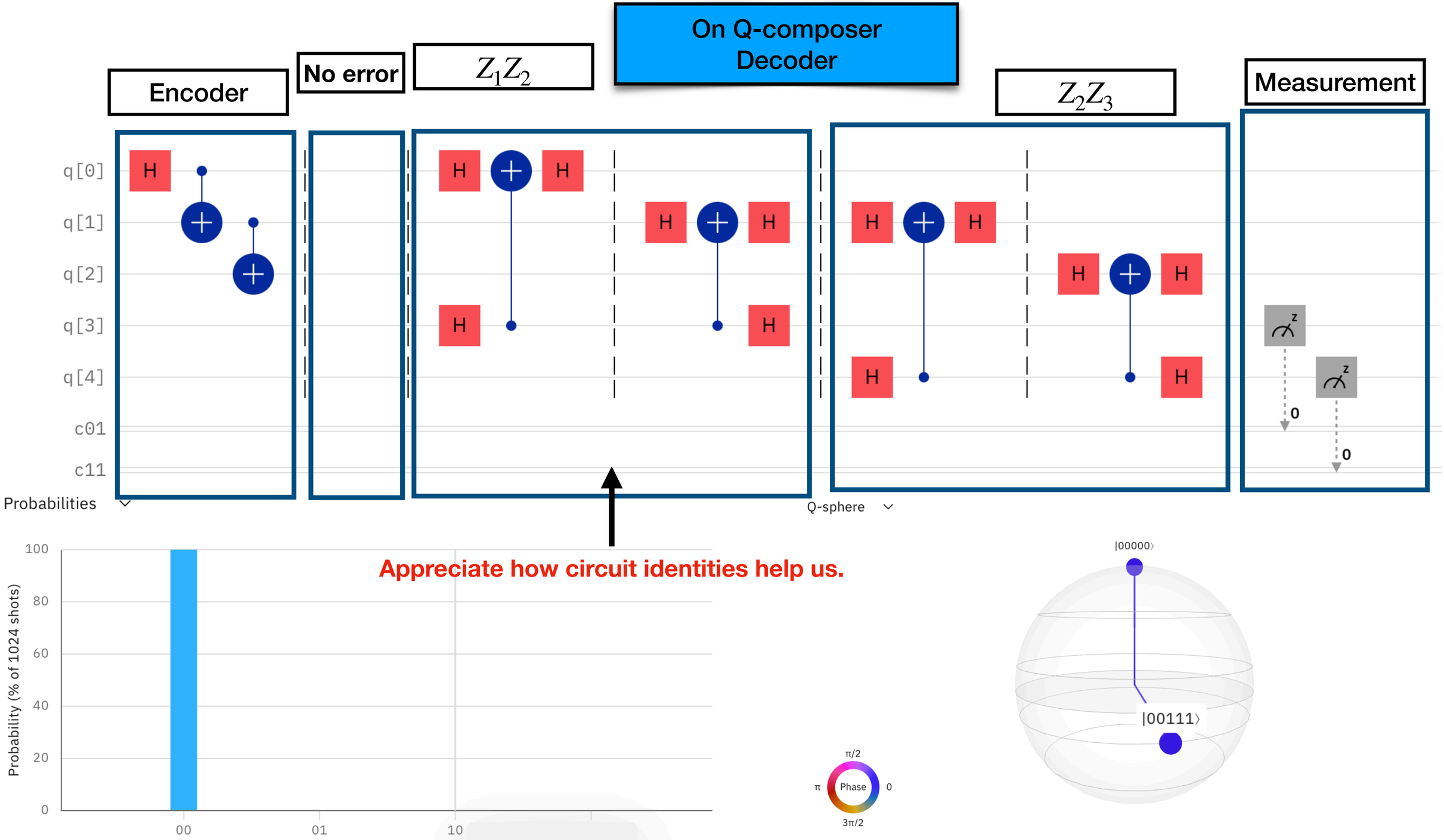
Probabilities

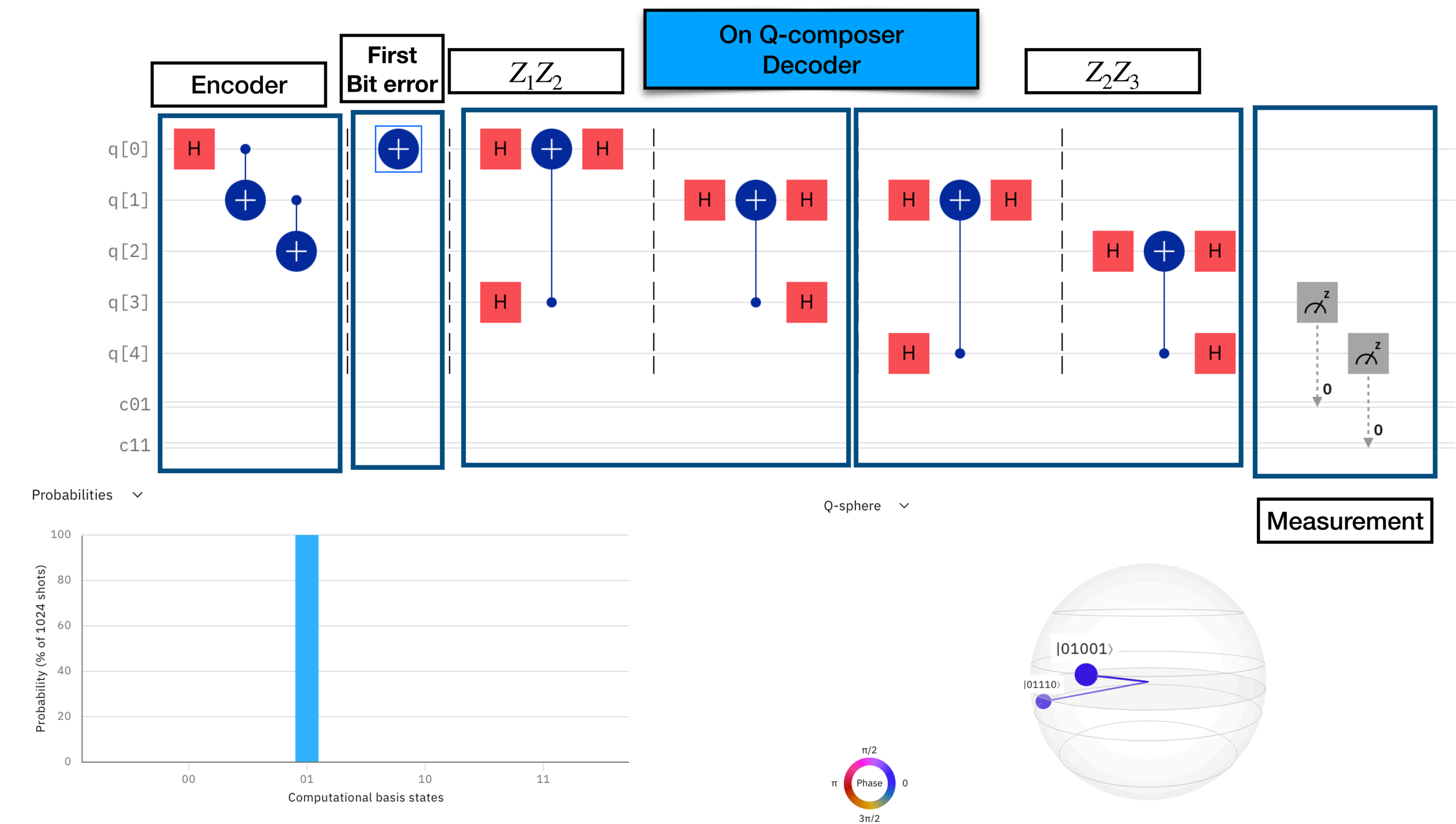
Q-sphere



Which state are we encoding?




On Q-composer
Decoder
Encoder
No error
Z_1Z_2
Z_2Z_3
Measurement
q[0]
q[1]
q[2]
q[3]
q[4]
c01
c11
H
0
0
Probabilities
Q-sphere
Appreciate how circuit identities help us.
100
80
60
40
20
0
Probability (% of 1024 shots)
00
01
10
|00000⟩
|00111⟩
π/2
π
Phase
0
3π/2

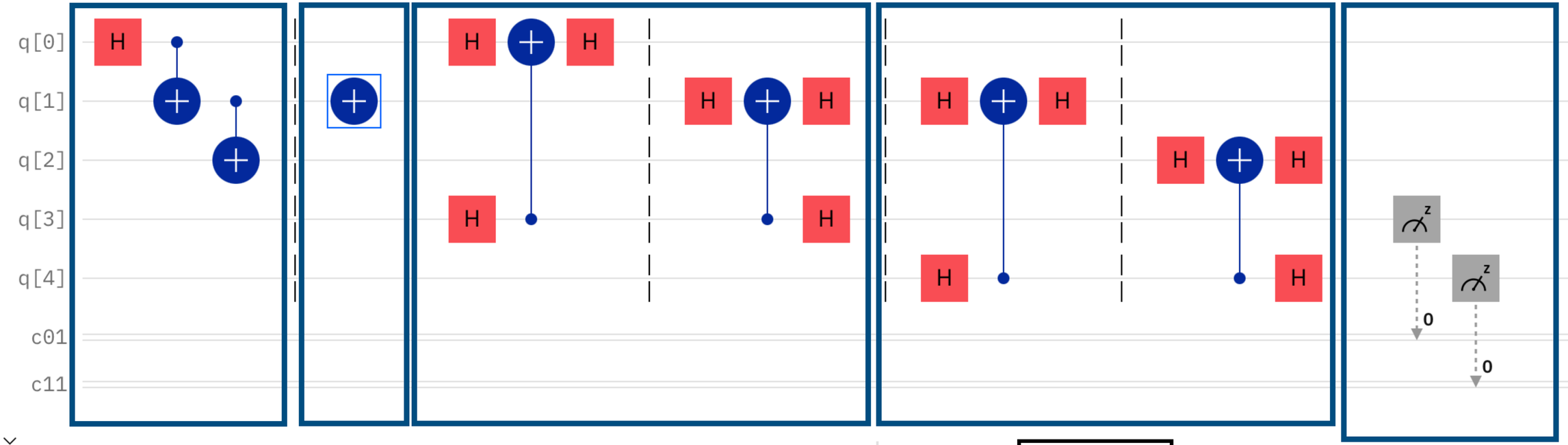

Encoder
First
Bit error
Z_1Z_2
On Q-composer
Decoder
Z_2Z_3
q[0]
q[1]
q[2]
q[3]
q[4]
c01
c11
H
Measurement
Probabilities
Q-sphere
100
80
60
40
20
0
Probability (% of 1024 shots)
00
01
10
11
Computational basis states
|01001⟩
|01110⟩
π/2
π
Phase
0
3π/2

Encoder

Second Bit error

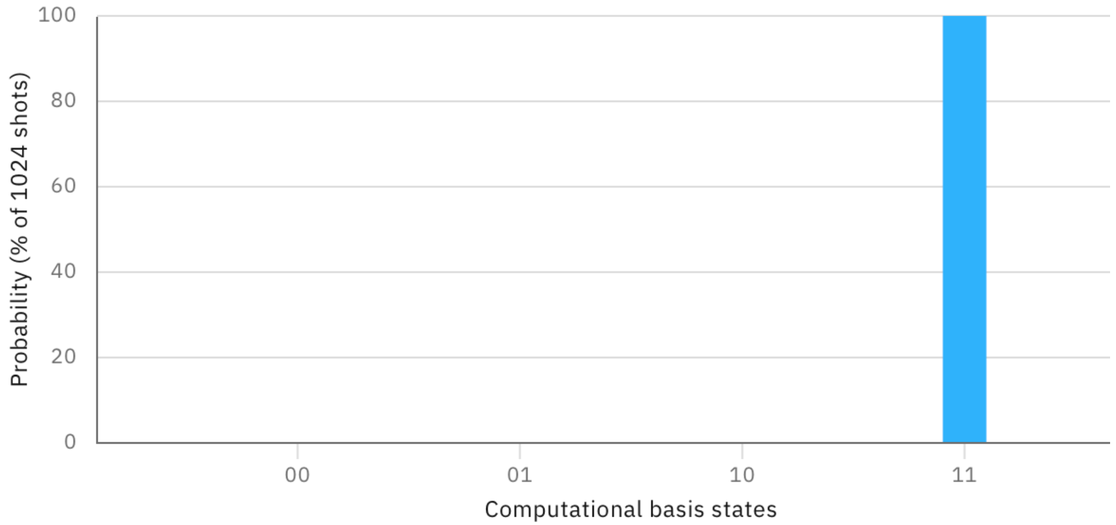
Z_1Z_2

On Q-composer Decoder



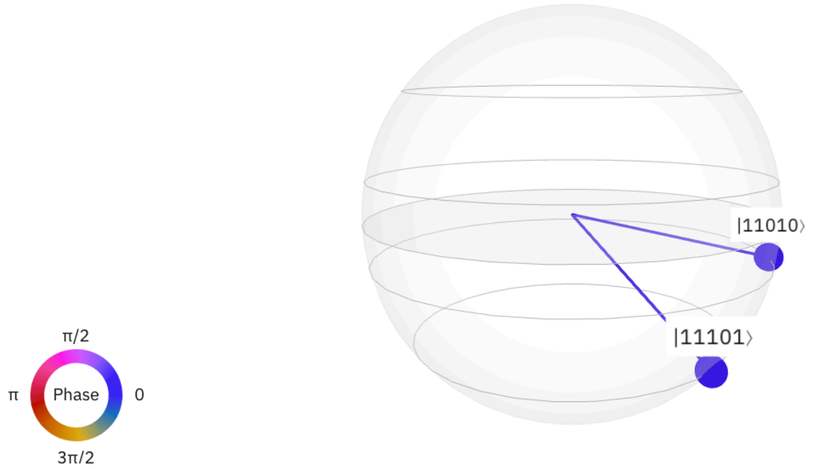
Measurement

Probabilities



Q-sphere

Z_2Z_3

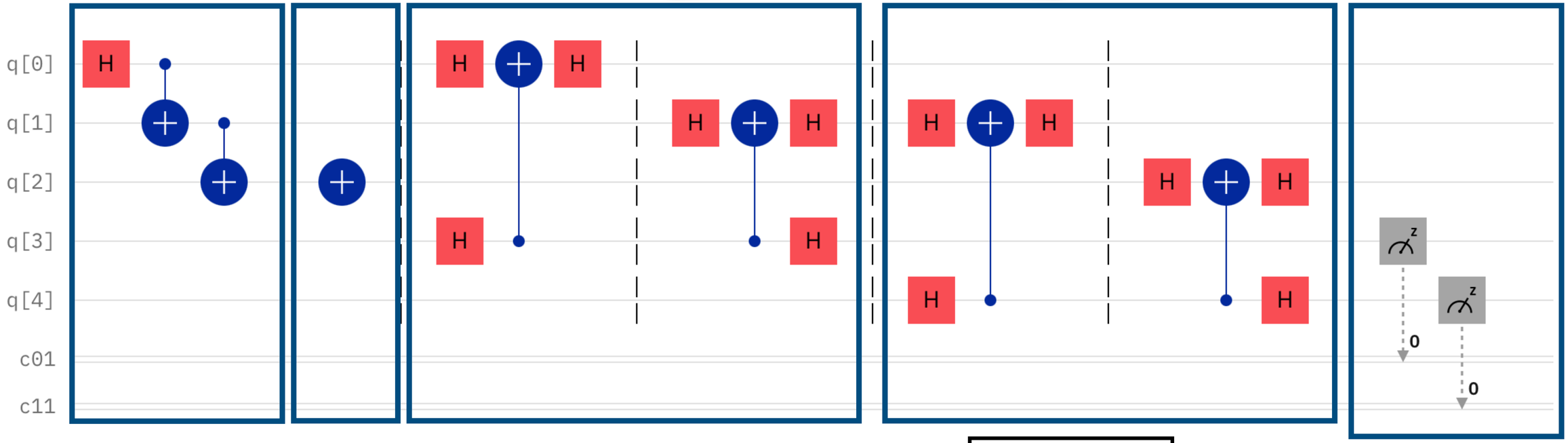


Encoder

Third Bit error

Z_1Z_2

On Q-composer Decoder

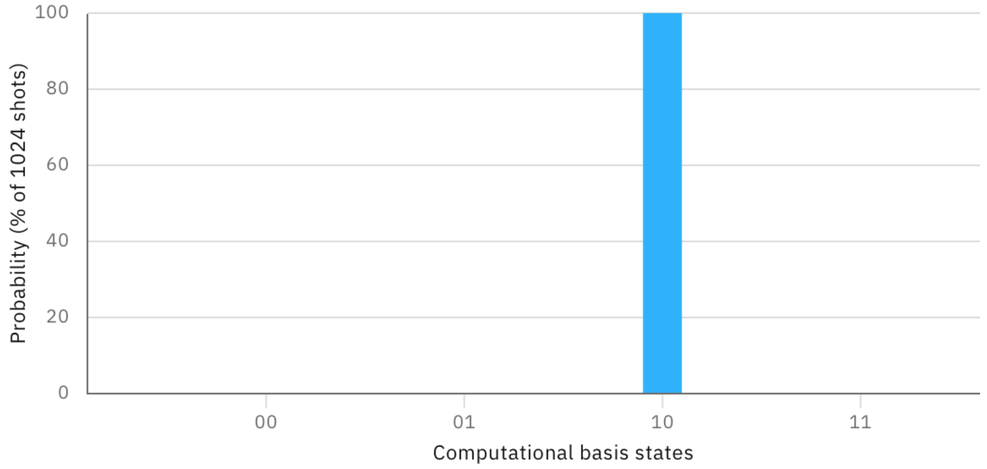


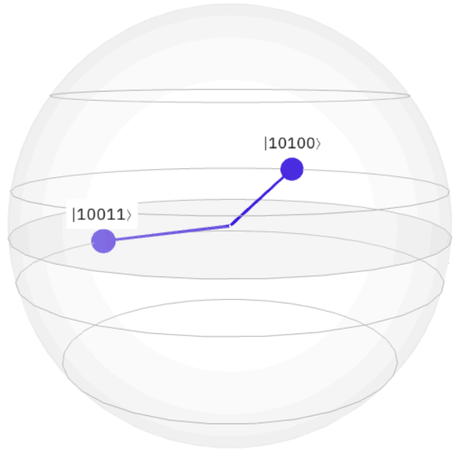
Q-sphere

Z_2Z_3

Measurement

Probabilities





Measure the Error, Not the Data

Information of the error syndrome $\Longrightarrow$ error or not

Measure the Error, Not the Data

Information of the error syndrome $\Longrightarrow$ error or not

Example: $\alpha|010\rangle + \beta|101\rangle$ has syndrome 11,

which means the second bit is different.

- Correct it with a X operation on the second qubit.

- Note that the syndrome does not depend on α and β.

Measure the Error, Not the Data

Information of the error syndrome $\Longrightarrow$ error or not

Example: $\alpha|010\rangle + \beta|101\rangle$ has syndrome 11,

which means the second bit is different.

- Correct it with a X operation on the second qubit.

- Note that the syndrome does not depend on α and β.

- Learned about the error without learning about the data, so superpositions are preserved!

What have we achieved?

- Failing probability ≡$p_u = 3p^2(1-p) + p^3 = 3p^2 - 2p^3 = O(p^2)$
- Fidelity ≡ success probability = $1 - p_u = 1 - 3p^2$
- Without error correction $p_u = O(p)$

Feature: Redundancy, Not Repetition

This encoding does not violate the no-cloning theorem:

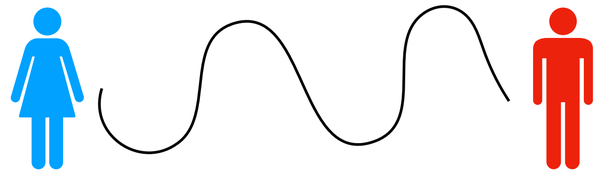
$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle \neq (\alpha|0\rangle + \beta|1\rangle)^{\otimes 3}$$

- Repeated the state only in the computational basis. Superposition states spread out (redundant encoding), but not repeated (which would violate no-cloning).

Resource?

Entanglement as a resource

$$\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)$$



Alice Bob

Z_A	Z_B
$+1$	$+1$
-1	-1

Entanglement

But

$$\frac{1}{2}\left(|0\rangle\langle 0| \, |0\rangle\langle 0| + |1\rangle\langle 1| \, |1\rangle\langle 1| \right)$$

Alice Bob

Z_A	Z_B
$+1$	$+1$
-1	-1

Same statistics!

Where is the difference?

What is this?
Mixed state?

Pure state

Identically independent distribution $|\psi\rangle$

Pure state

Identically independent distribution $|\psi\rangle$

Mixed state

Identically independent distribution

$$p_1, |\psi_1\rangle$$
$$p_2, |\psi_2\rangle$$
$$p_3, |\psi_3\rangle$$
$$\vdots$$

Pure state

Identically independent distribution $|\psi\rangle$

Mixed state

Identically independent distribution

$$p_1, |\psi_1\rangle$$
$$p_2, |\psi_2\rangle$$
$$p_3, |\psi_3\rangle$$
$$\vdots$$

Mathematically represented as $p_1 |\psi_1\rangle\langle\psi_1| + p_2 |\psi_2\rangle\langle\psi_2| + \cdots$

Density matrix

An operator ρ is said to be a density operator if:

(1) $\rho^\dagger = \rho$

(2) $\mathrm{tr}\ \rho = 1$

(3) ρ is a non-negative operator.

$\rho^2 = \rho \implies$ Pure state

$\rho^2 \neq \rho \implies$ Not a pure state

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

Example

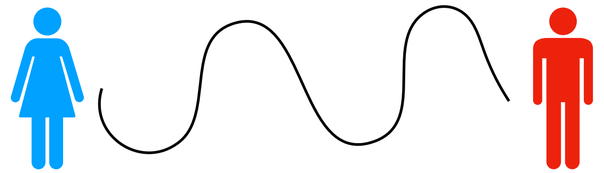
1. $0.2\,|0\rangle\langle 0| + 0.8\,|1\rangle\langle 1|$

2. $p\,|0\rangle\langle 0| + (1-p)\,|1\rangle\langle 1|$

Entanglement

$$\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)$$

$$= \frac{1}{\sqrt{2}}\left(|+\rangle_A|+\rangle_B + |-\rangle_A|-\rangle_B\right)$$



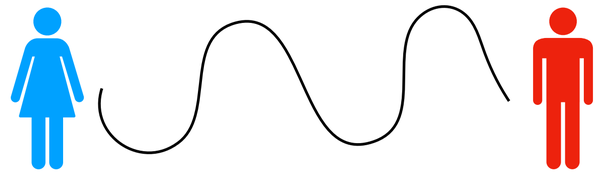
Alice Bob

$$|\pm\rangle \equiv \frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right)$$

Entanglement

$$\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)$$

$$= \frac{1}{\sqrt{2}}\left(|+\rangle_A|+\rangle_B + |-\rangle_A|-\rangle_B\right)$$



Alice Bob

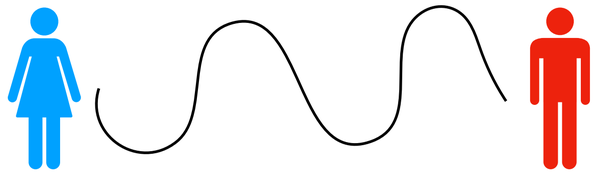
Verify it!

$$|\pm\rangle \equiv \frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right)$$

Entanglement

$$\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)$$

$$= \frac{1}{\sqrt{2}}\left(|+\rangle_A|+\rangle_B + |-\rangle_A|-\rangle_B\right)$$



Alice Bob

$$|\pm\rangle \equiv \frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right)$$

X_A	X_B
$+1$	$+1$
-1	-1

Entanglement

However $\frac{1}{2}\left(|0\rangle\langle 0| \, |0\rangle\langle 0| + |1\rangle\langle 1| \, |1\rangle\langle 1| \right)$

Alice Bob

$$\neq \frac{1}{2}\left(|+\rangle\langle +| \, |+\rangle\langle +| + |-\rangle\langle -| \, |-\rangle\langle -| \right)$$

X_A	X_B
$+1$	$+1$
-1	-1
$\vdots$	$\vdots$

Same statistics!

PAUSE

ANY Questions??

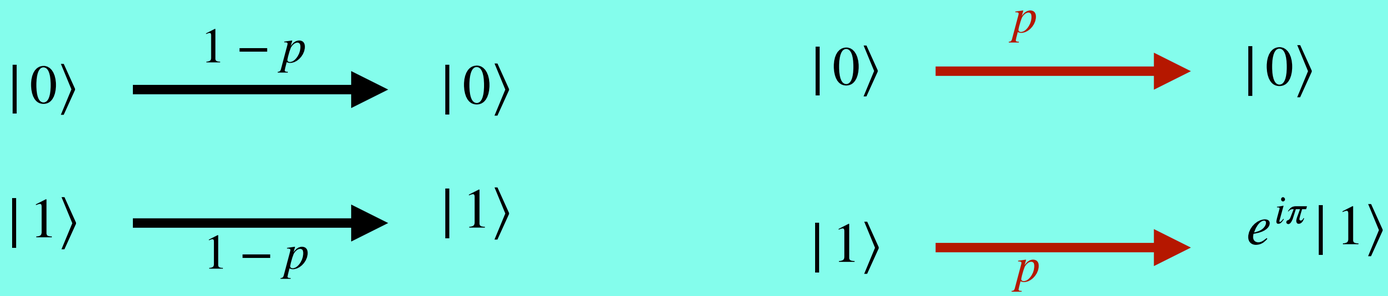
Other noisy channels

Bit-flip channel:

Other noisy channels

Bit-flip channel:

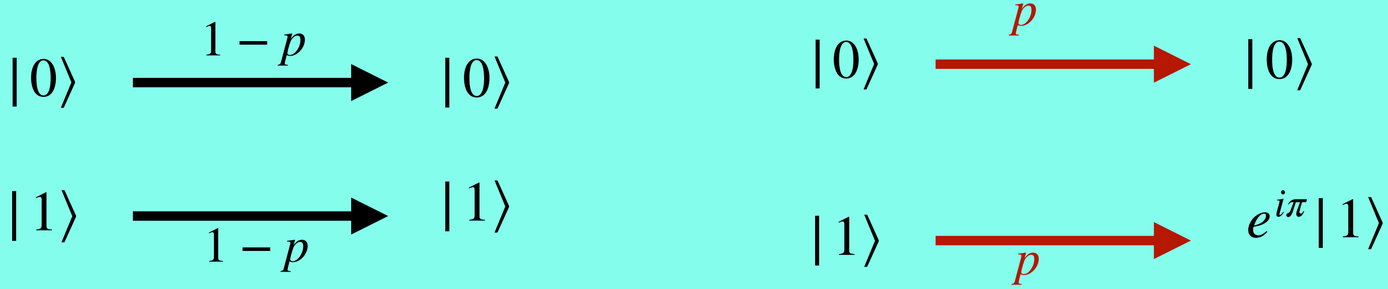
Phase-flip channel:



Other noisy channels

Bit-flip channel:

Phase-flip channel:



Bit+Phase-flip channel:

Quantum Error Correction: Requirements

1. Must correct multiple types of errors (e.g., bit flip and phase errors).
2. How can we correct continuous errors and decoherence?

Correcting Just Phase Errors

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$Z|0\rangle = |0\rangle, \qquad Z|1\rangle = e^{i\pi}|1\rangle$$

$$Z\big(\alpha|0\rangle + \beta|1\rangle\big) = \alpha|0\rangle - \beta|1\rangle$$

Correcting Just Phase Errors

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$Z|0\rangle = |0\rangle, \qquad Z|1\rangle = e^{i\pi}|1\rangle$$

$$\boxed{Z\big(\alpha|0\rangle + \beta|1\rangle\big) = \alpha|0\rangle - \beta|1\rangle}$$

$$H(\alpha|0\rangle + \beta|1\rangle) = \alpha|+\rangle + \beta|-\rangle$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H|0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \equiv |+\rangle$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) \equiv |-\rangle$$

Correcting Just Phase Errors

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$Z|0\rangle = |0\rangle, \qquad Z|1\rangle = e^{i\pi}|1\rangle$$

$$Z\big(\alpha|0\rangle + \beta|1\rangle\big) = \alpha|0\rangle - \beta|1\rangle$$

$$H(\alpha|0\rangle + \beta|1\rangle) = \alpha|+\rangle + \beta|-\rangle$$

$$Z|+\rangle = |-\rangle \qquad Z|-\rangle = |+\rangle$$

Just like bit-flip in Hadamard basis

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H|0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \equiv |+\rangle$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) \equiv |-\rangle$$

Correcting Just Phase Errors

$$Z\big(\alpha|0\rangle + \beta|1\rangle\big) = \alpha|0\rangle - \beta|1\rangle$$

$$H(\alpha|0\rangle + \beta|1\rangle) = \alpha|+\rangle + \beta|-\rangle$$

$$Z|+\rangle = |-\rangle \qquad Z|-\rangle = |+\rangle$$

$X|\pm\rangle = \pm|\pm\rangle$ (acts like phase flip)

$Z|\pm\rangle = |\mp\rangle$ (acts like bit flip)

Verify it!

Correcting Just Phase Errors

$$Z\big(\alpha|0\rangle+\beta|1\rangle\big)=\alpha|0\rangle-\beta|1\rangle$$

$$H(\alpha|0\rangle+\beta|1\rangle)=\alpha|+\rangle+\beta|-\rangle$$

$$Z|+\rangle=|-\rangle \qquad Z|-\rangle=|+\rangle$$

$X|\pm\rangle=\pm|\pm\rangle$ (acts like phase flip)

$Z|\pm\rangle=|\mp\rangle$ (acts like bit flip)

Hadamard transform H exchanges bit flip and phase errors.

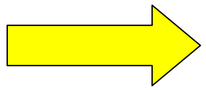
What if we exchange the roles of two?

Can the same code correct phase-flips with small modification?

Yes!

Correcting Just Phase Errors

Repetition code corrects a bit flip error

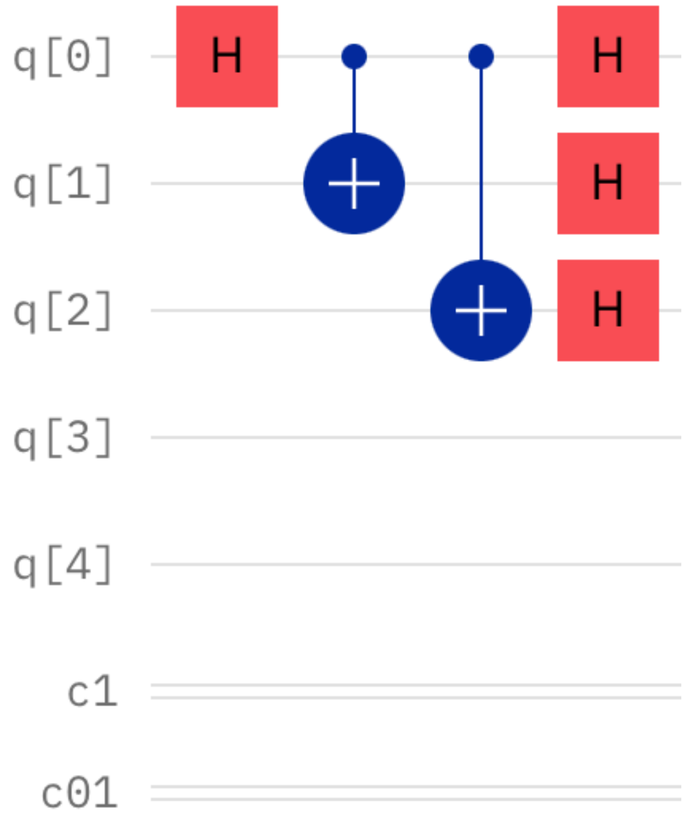


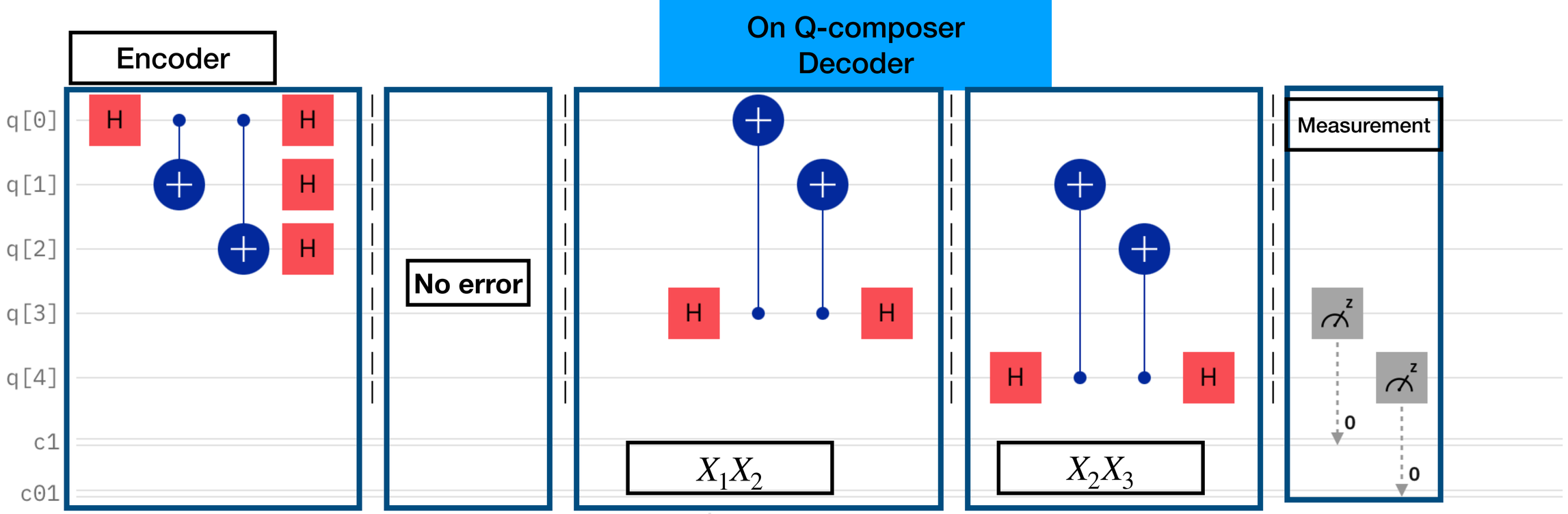
Repetition code in Hadamard basis corrects a phase error.

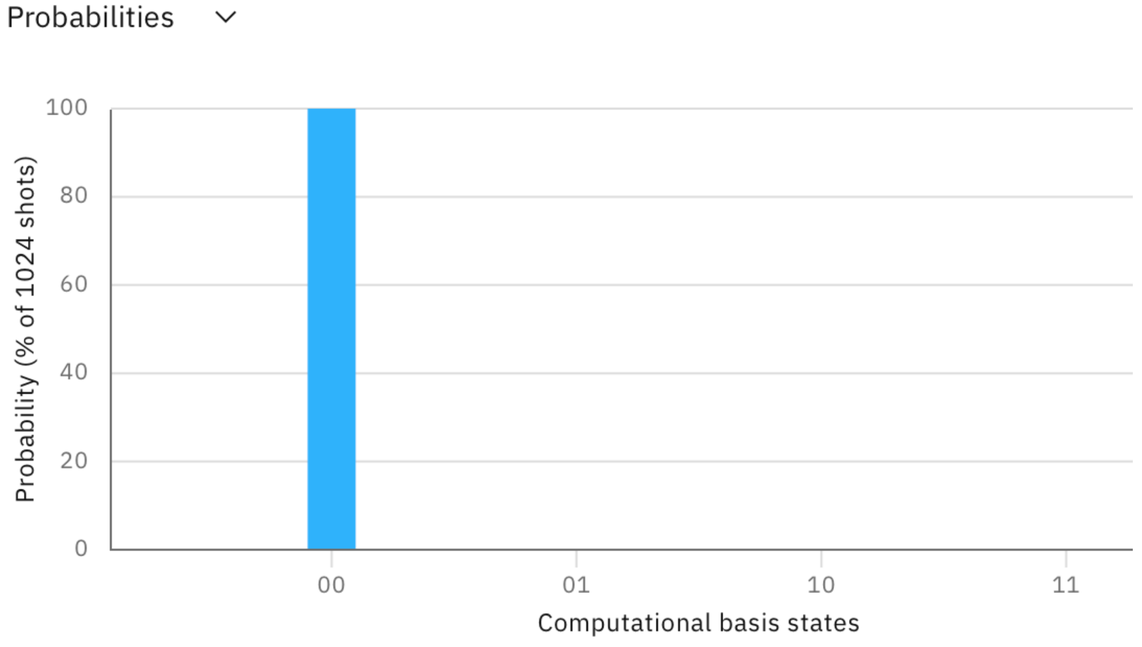
$$\alpha|+\rangle+\beta|-\rangle \rightarrow \alpha|+++\rangle+\beta|---\rangle$$

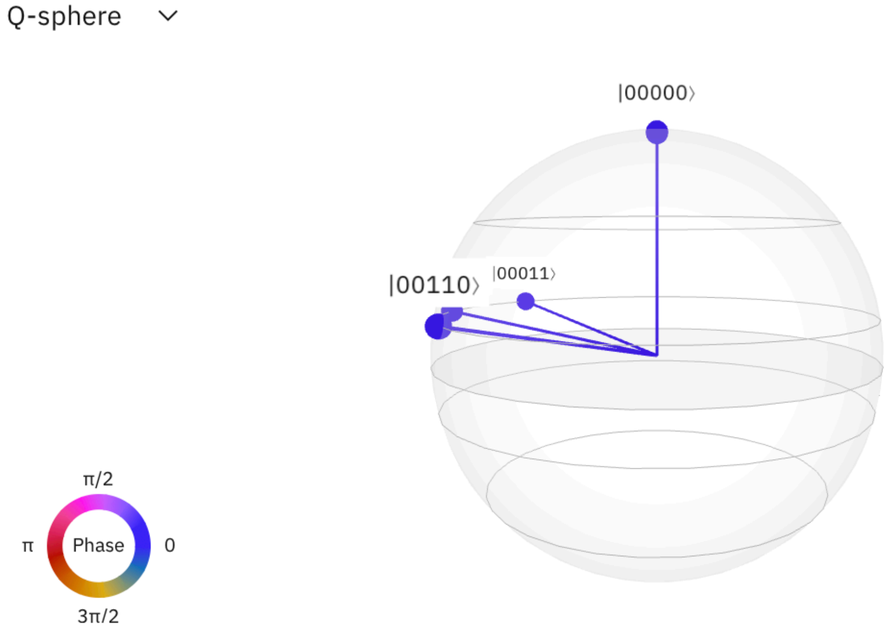
Exercise: Work out the syndrome measurements and correction procedure for three-qubit phase flip code.

On Q-composer
Generation of a logical state

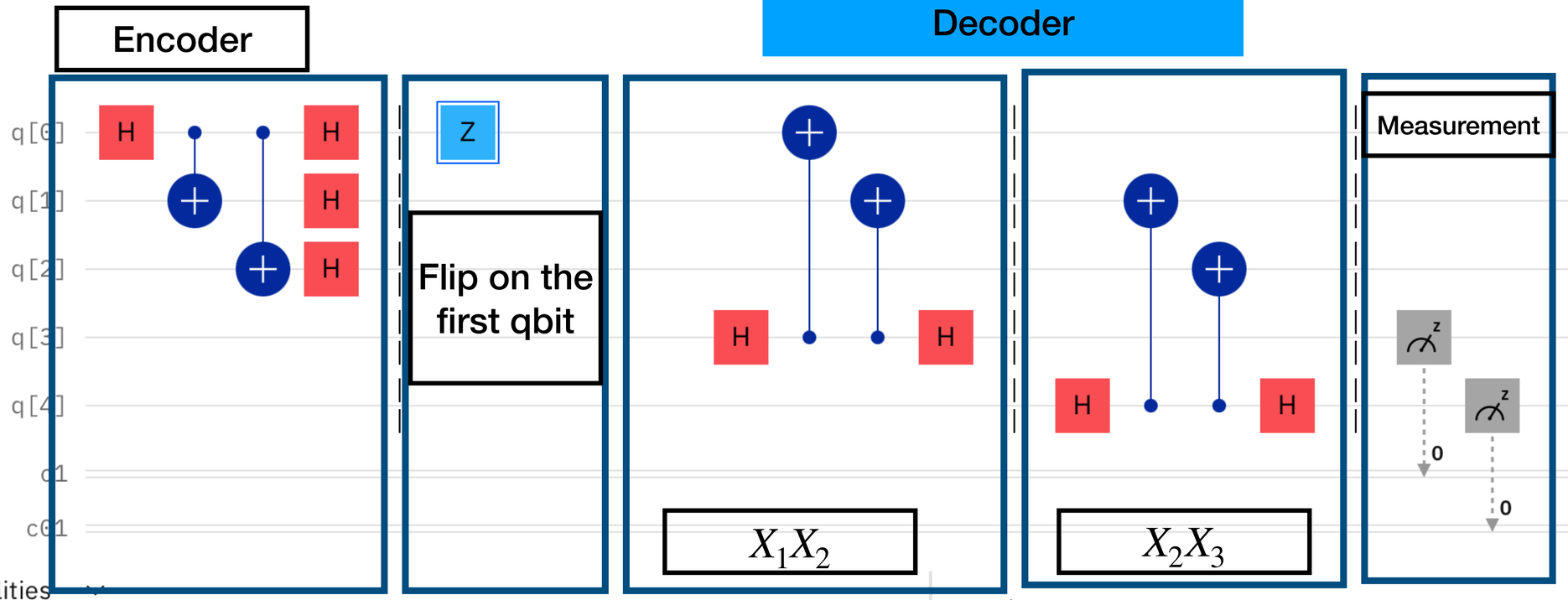



Encoder
On Q-composer
Decoder
q[0]
q[1]
q[2]
q[3]
q[4]
c1
c01
H
No error
X_1X_2
X_2X_3
Measurement
0
0

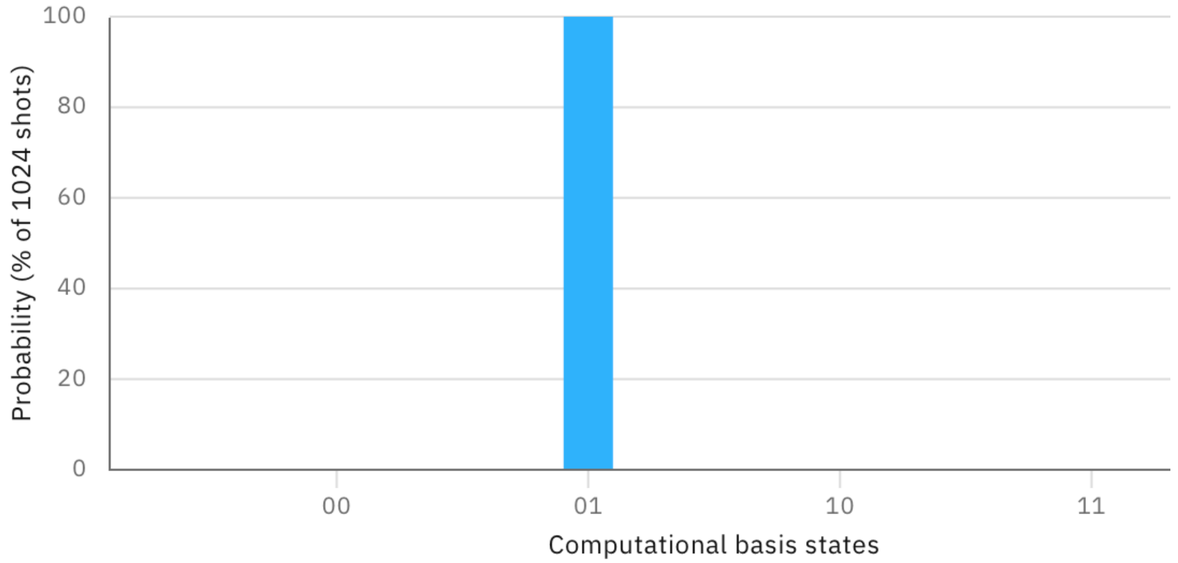

Probabilities
100
80
60
40
20
0
Probability (% of 1024 shots)
00
01
10
11
Computational basis states


Q-sphere
|00000⟩
|00110⟩
|00011⟩
π/2
π
Phase
0
3π/2

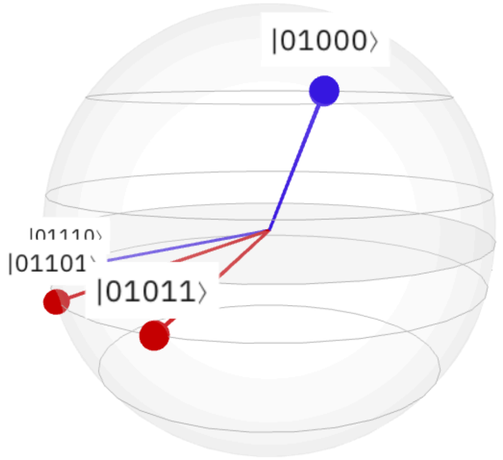
On Q-composer
Decoder

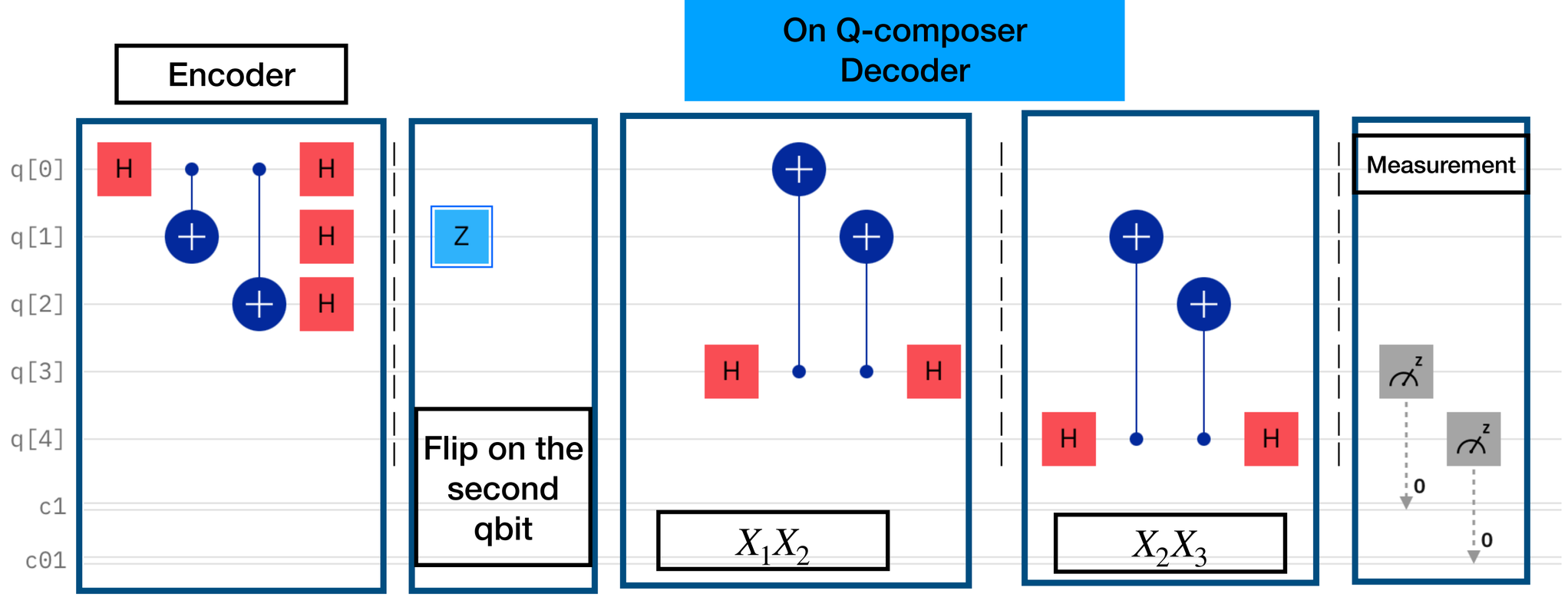


Probabilities

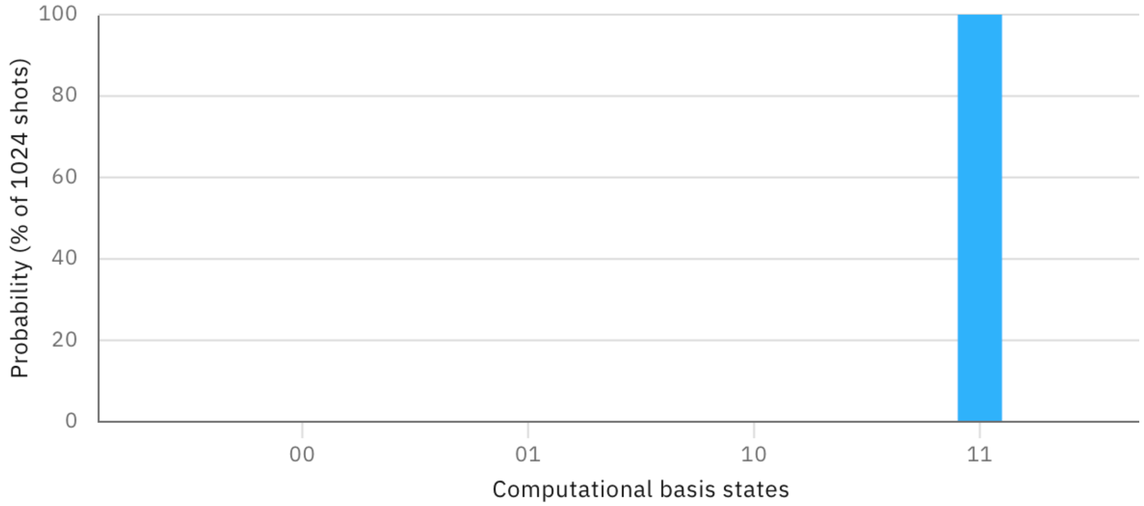


Q-sphere

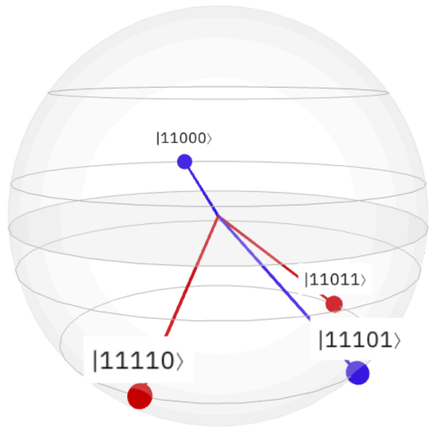




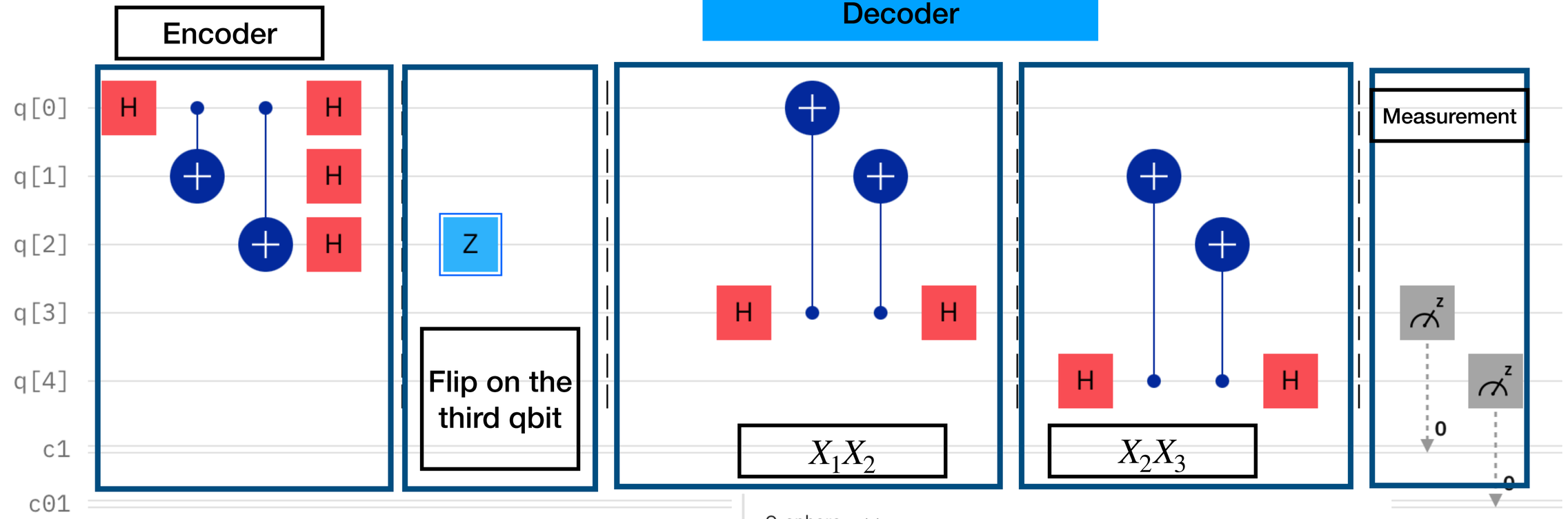
Probabilities



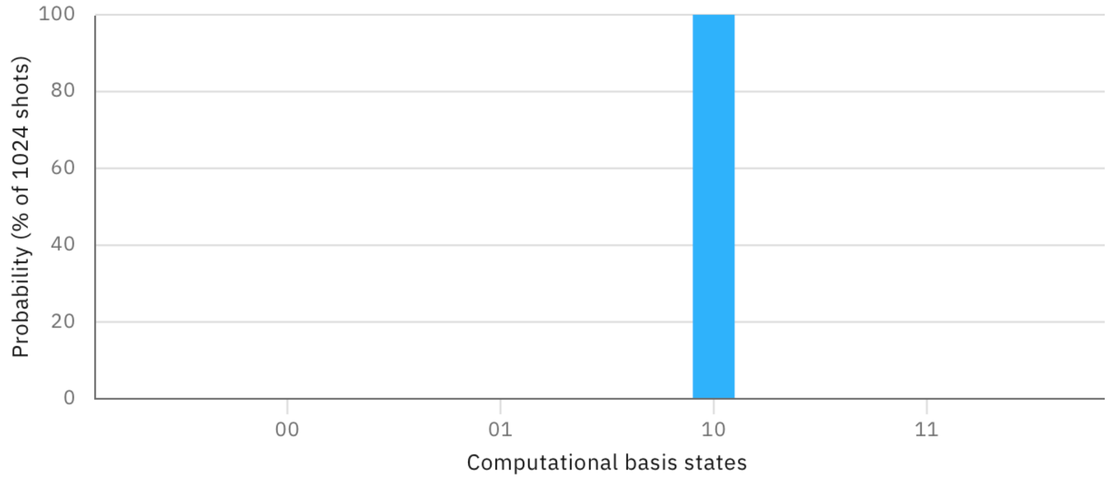
Q-sphere



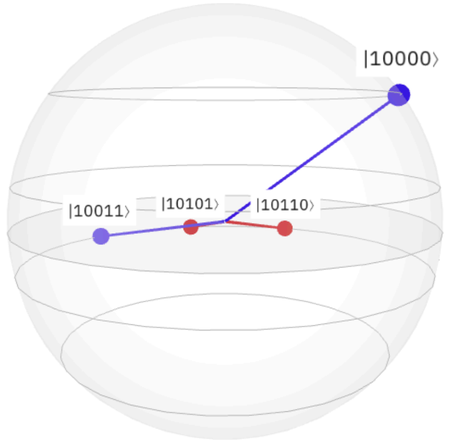
On Q-composer
Decoder



Probabilities



Q-sphere



General error

- Errors occur due to interaction with environment

General error

- Errors occur due to interaction with environment

$$|0\rangle|E\rangle \rightarrow \beta_1|0\rangle|E_1\rangle + \beta_2|1\rangle|E_2\rangle$$

$$|1\rangle|E\rangle \rightarrow \beta_3|1\rangle|E_3\rangle + \beta_4|0\rangle|E_4\rangle$$

General error

- Errors occur due to interaction with environment

$$|0\rangle|E\rangle \rightarrow \beta_1|0\rangle|E_1\rangle + \beta_2|1\rangle|E_2\rangle$$

$$|1\rangle|E\rangle \rightarrow \beta_3|1\rangle|E_3\rangle + \beta_4|0\rangle|E_4\rangle$$

$$(\alpha_0|0\rangle + \alpha_1|1\rangle)|E\rangle \rightarrow \alpha_0\beta_1|0\rangle|E_1\rangle + \alpha_0\beta_2|1\rangle|E_2\rangle + \alpha_1\beta_3|1\rangle|E_3\rangle + \alpha_1\beta_4|0\rangle|E_4\rangle$$

General error

$$(\alpha_0|0\rangle + \alpha_1|1\rangle)|E\rangle \to \frac{1}{2}(\alpha_0|0\rangle + \alpha_1|1\rangle)(\beta_1|E_1\rangle + \beta_3|E_3\rangle)$$
$$+\frac{1}{2}(\alpha_0|0\rangle - \alpha_1|1\rangle)(\beta_1|E_1\rangle - \beta_3|E_3\rangle)$$
$$+\frac{1}{2}(\alpha_0|1\rangle + \alpha_1|0\rangle)(\beta_2|E_2\rangle + \beta_4|E_4\rangle)$$
$$+\frac{1}{2}(\alpha_0|1\rangle - \alpha_1|0\rangle)(\beta_2|E_1\rangle - \beta_4|E_4\rangle)$$

$$\alpha_0|0\rangle + \alpha_1|1\rangle = |\psi\rangle$$
$$\alpha_0|0\rangle - \alpha_1|1\rangle = Z|\psi\rangle$$
$$\alpha_0|1\rangle + \alpha_1|0\rangle = X|\psi\rangle$$
$$\alpha_0|1\rangle - \alpha_1|0\rangle = XZ|\psi\rangle$$

Exercise: Do it!!!

General error

$$(\alpha_0|0\rangle + \alpha_1|1\rangle)|E\rangle \rightarrow \frac{1}{2}|\psi\rangle(\beta_1|E_1\rangle + \beta_3|E_3\rangle)$$
$$+\frac{1}{2}Z|\psi\rangle(\beta_1|E_1\rangle - \beta_3|E_3\rangle)$$
$$+\frac{1}{2}X|\psi\rangle(\beta_2|E_2\rangle + \beta_4|E_4\rangle)$$
$$+\frac{1}{2}XZ|\psi\rangle(\beta_2|E_1\rangle - \beta_4|E_4\rangle)$$

- Error basis = I, X, Z, XZ

General error

$$(\alpha_0|0\rangle + \alpha_1|1\rangle)|E\rangle \rightarrow \frac{1}{2}|\psi\rangle(\beta_1|E_1\rangle + \beta_3|E_3\rangle)$$
$$+\frac{1}{2}Z|\psi\rangle(\beta_1|E_1\rangle - \beta_3|E_3\rangle)$$
$$+\frac{1}{2}X|\psi\rangle(\beta_2|E_2\rangle + \beta_4|E_4\rangle)$$
$$+\frac{1}{2}XZ|\psi\rangle(\beta_2|E_1\rangle - \beta_4|E_4\rangle)$$

- Error basis = I, X, Z, XZ
- $|\psi\rangle_L|\varphi\rangle_e \rightarrow \Sigma(\varepsilon_i|\psi\rangle_L)|\varphi_i\rangle_e$
- $|\psi\rangle_L \equiv$ general superposition of quantum codewords
- $\varepsilon_i \equiv$ error operator = tensor product of pauli operators

General error

$$|\psi\rangle_L |\phi\rangle_e \rightarrow \sum \left(\epsilon_i |\psi\rangle_L\right) |\phi_i\rangle$$

$|\psi\rangle_i \equiv$ Orthonormal set of n qubit states

To extract syndrome attach an $n-k$ qubit Ancilla “a” to system $\rightarrow$ perform operations to get syndrome $\equiv |s_i\rangle_a$

$$\Longrightarrow \ |0\rangle_a \sum \left(\epsilon_i |\psi\rangle_L\right) |\phi_i\rangle_e \rightarrow \sum |s_i\rangle_a \left(|\psi\rangle_L\right) |\phi_i\rangle_e$$

Measure s_i to determine $\epsilon^{-1} \rightarrow$ Correct the error

$$\Longrightarrow \ |s_i\rangle_a \left(\epsilon_i |\psi\rangle_L\right) |\phi_i\rangle_e \rightarrow |s_i\rangle_a \left(|\psi\rangle_L\right) |\phi_i\rangle_e$$

An explicit example: Nine qubit code

Nine-Qubit Code

To correct both bit flips and phase flips, use both codes at once, i.e.,

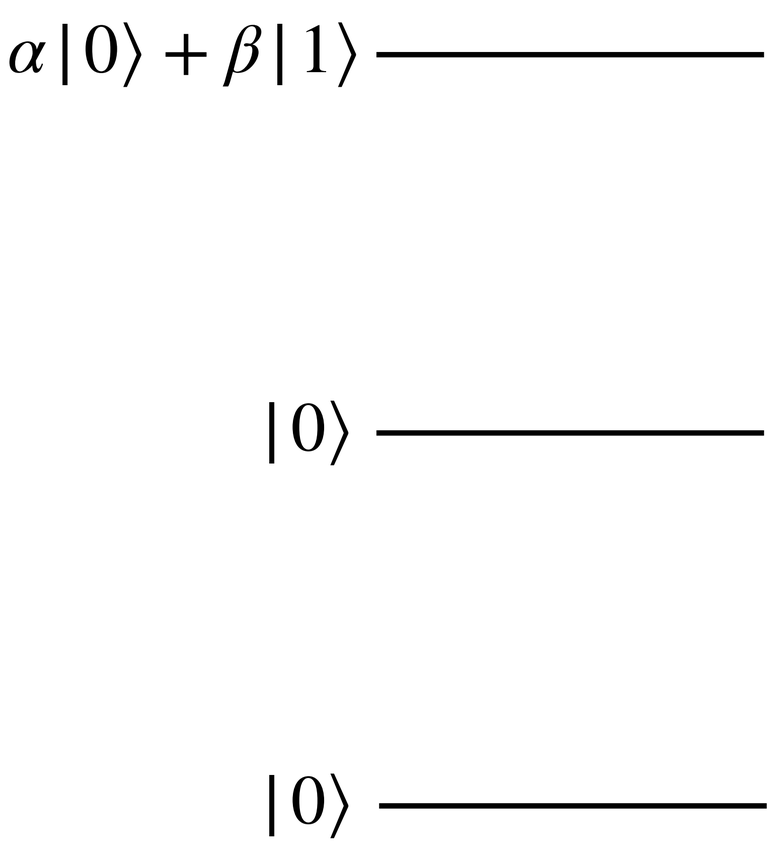
$$\alpha|0\rangle+\beta|1\rangle \rightarrow \alpha\Big(|000\rangle+|111\rangle\Big)^{\otimes 3}+\beta\Big(|000\rangle-|111\rangle\Big)^{\otimes 3}$$

Repetition 000, 111 corrects a bit flip error, repetition of phase +++, --- corrects a phase error

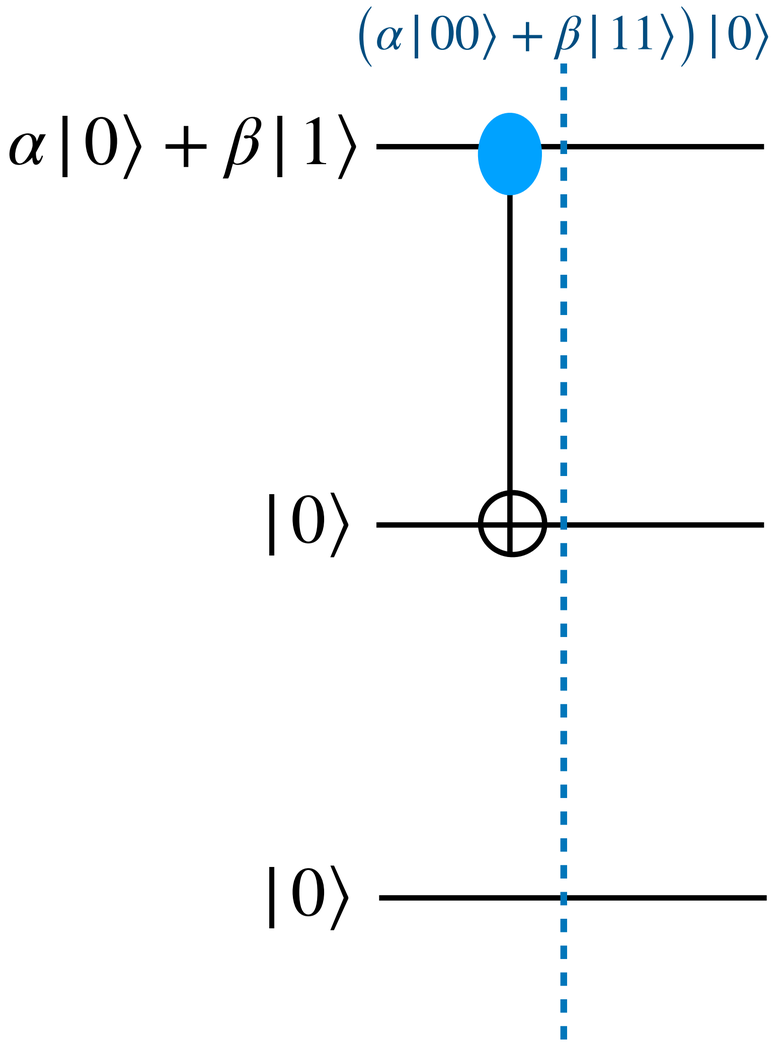
This code corrects a bit flip and a phase, so it also corrects a Y error:

$$Y=iXZ:\ Y|0\rangle=i|1\rangle, Y|1\rangle=-i|0\rangle$$ (global phase irrelevant)

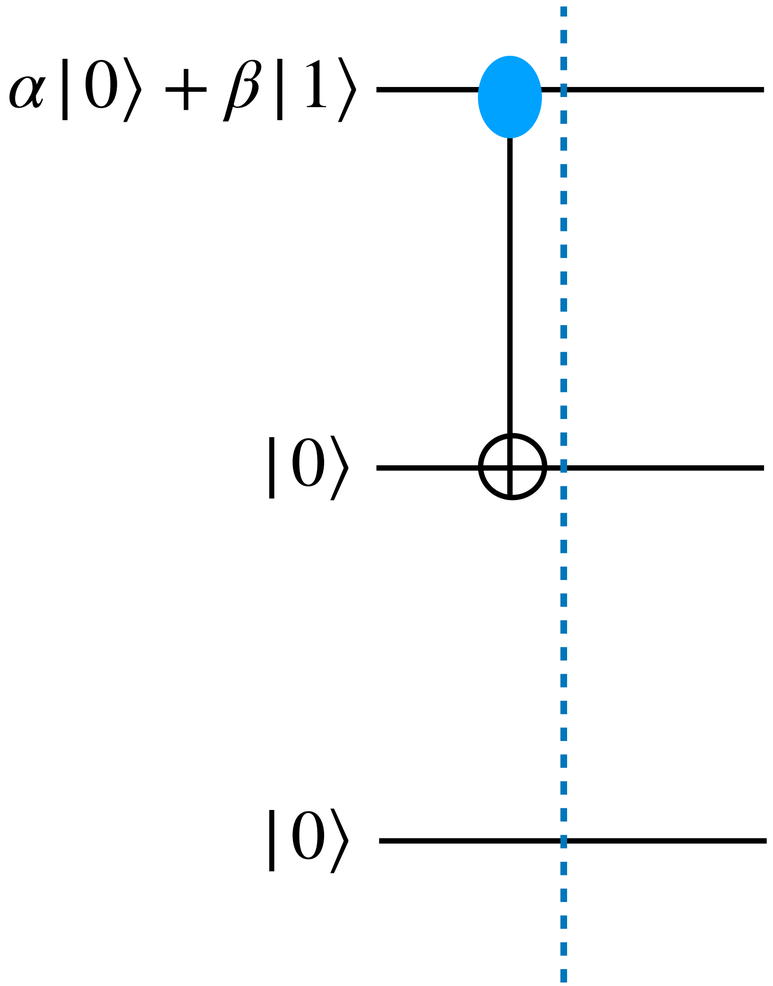
Circuit for a nine-qubit code



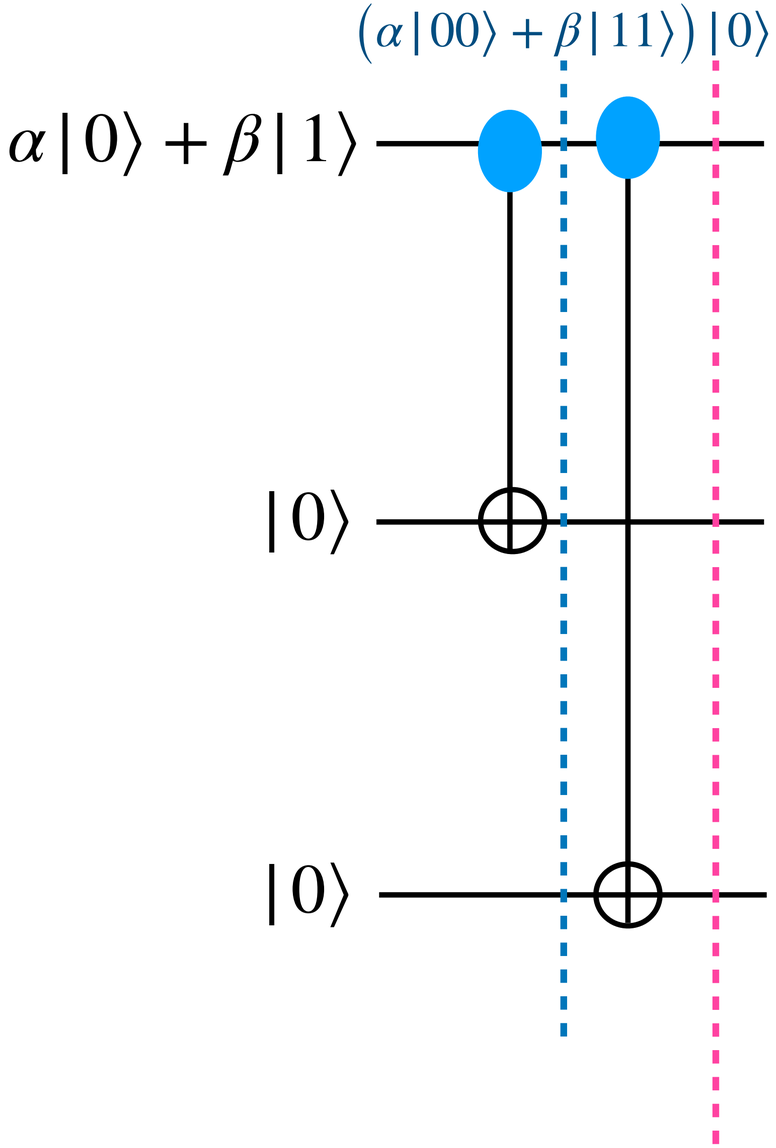
Circuit for a nine-qubit code



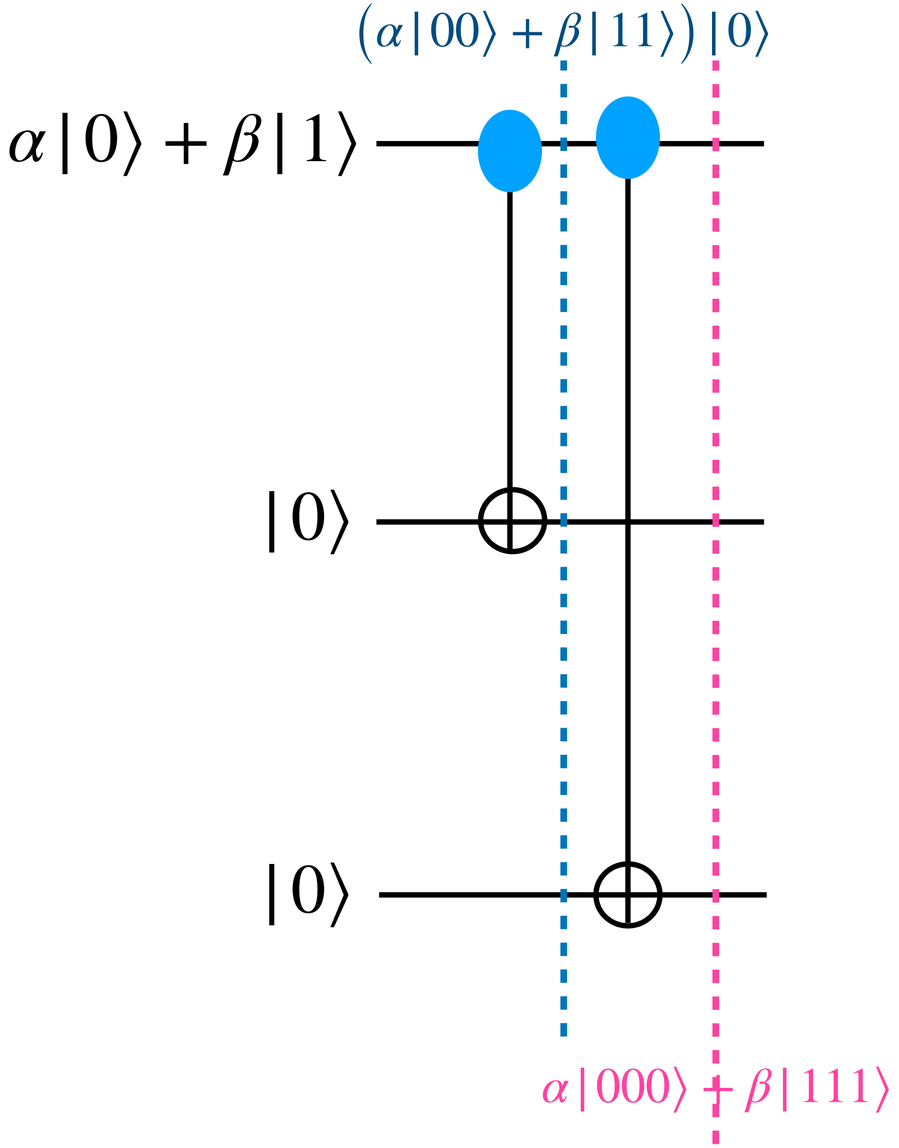
Circuit for a nine-qubit code



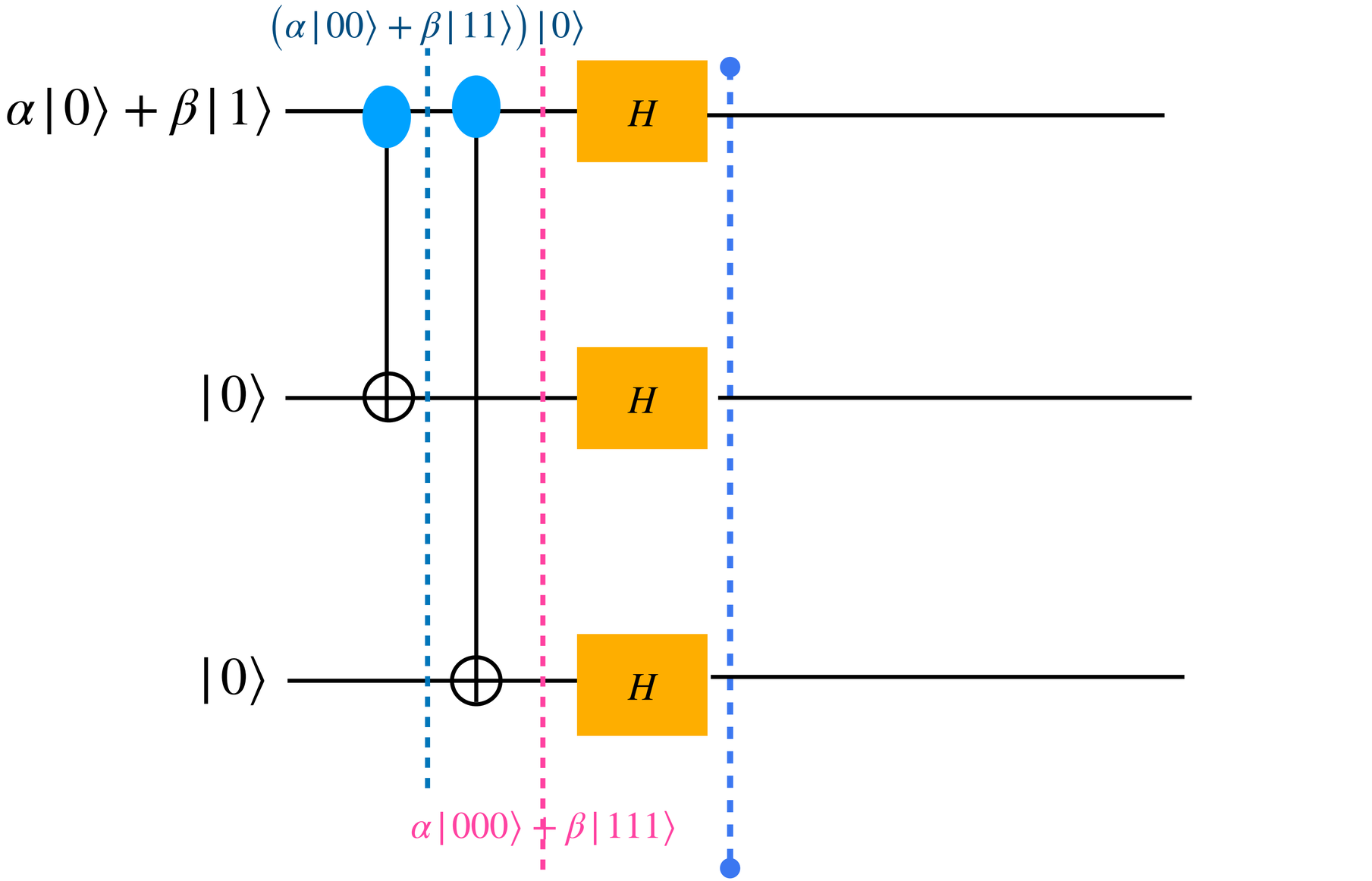
Circuit for a nine-qubit code



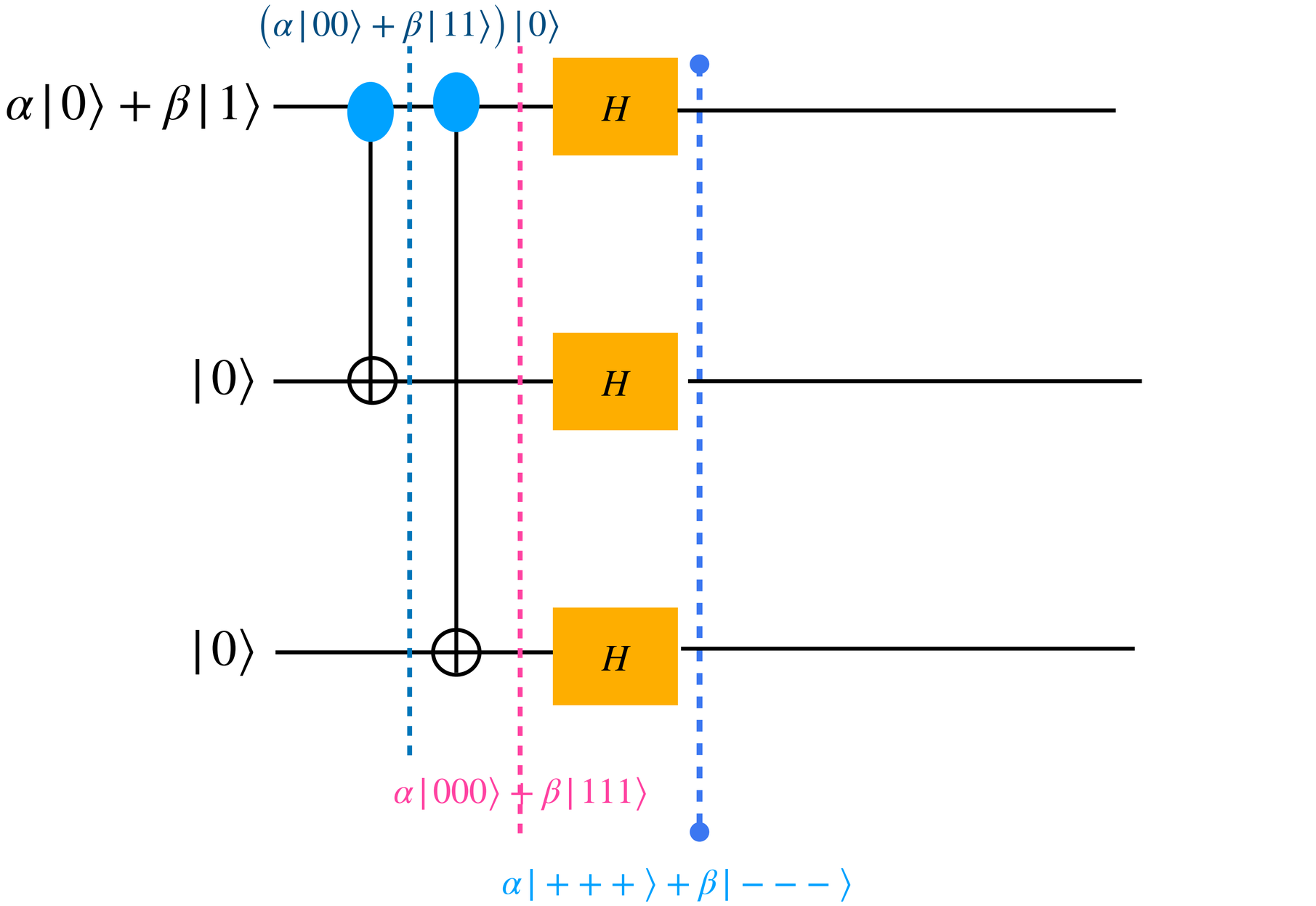
Circuit for a nine-qubit code



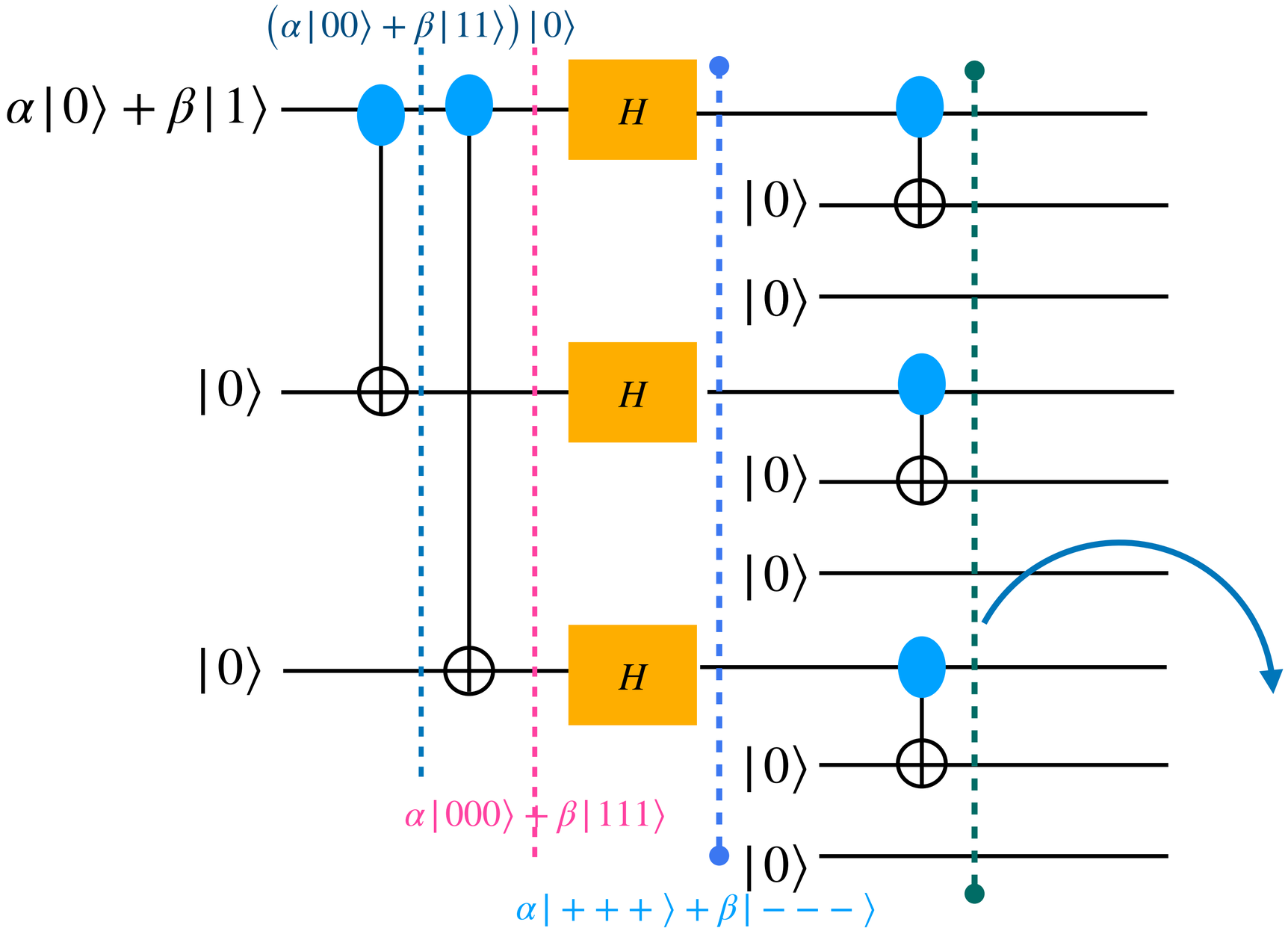
Circuit for a nine-qubit code



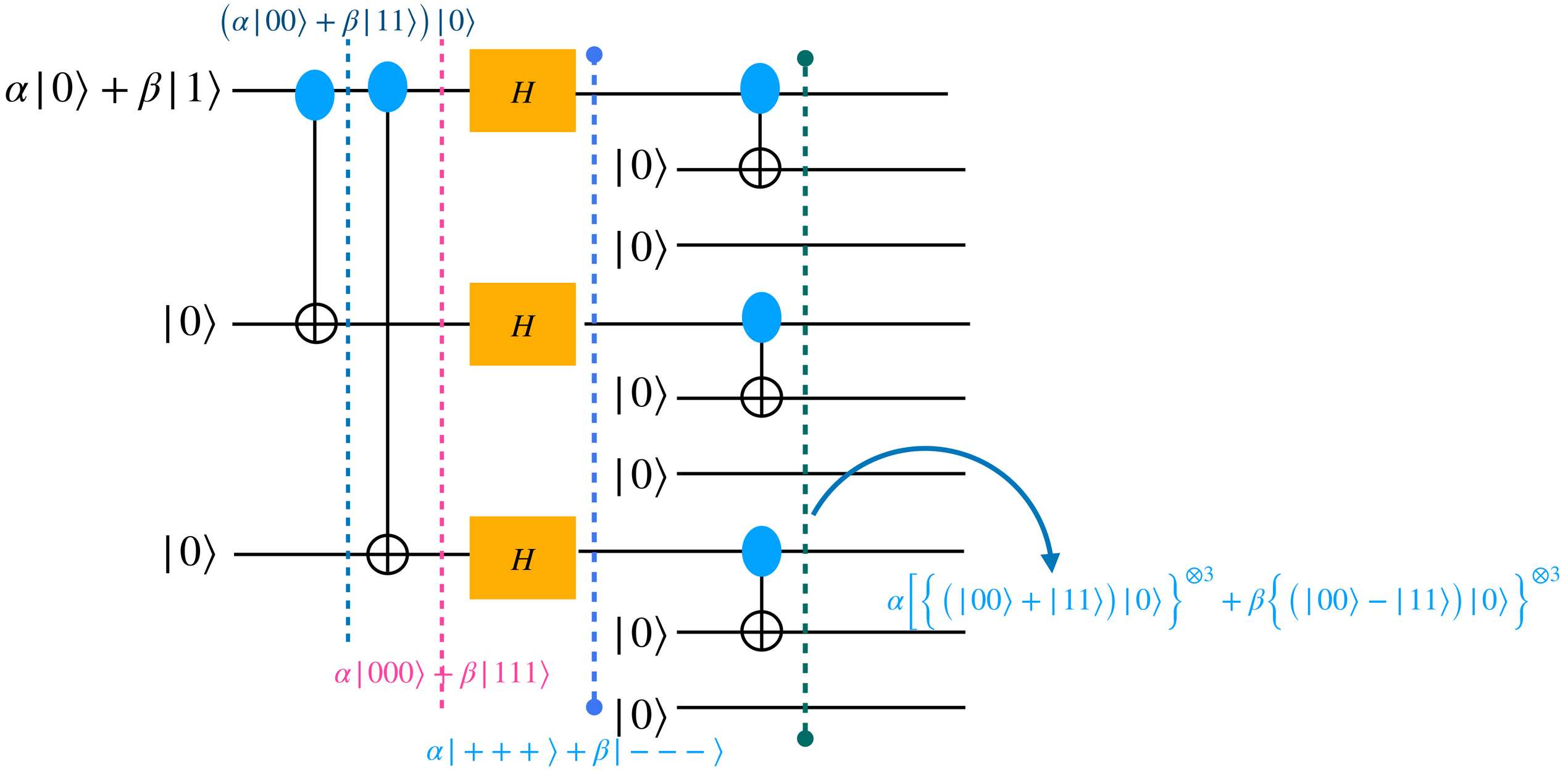
Circuit for a nine-qubit code



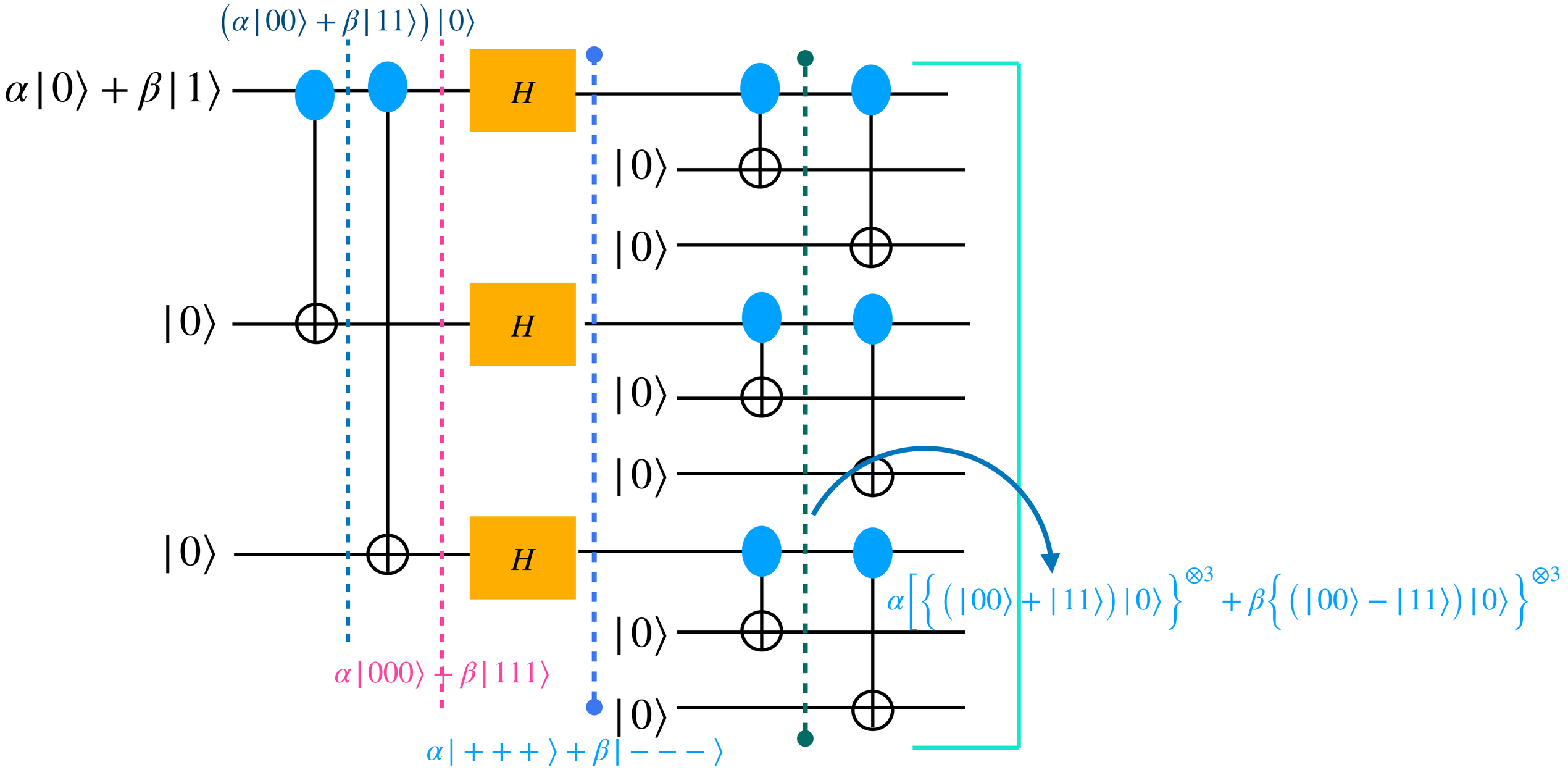
Circuit for a nine-qubit code

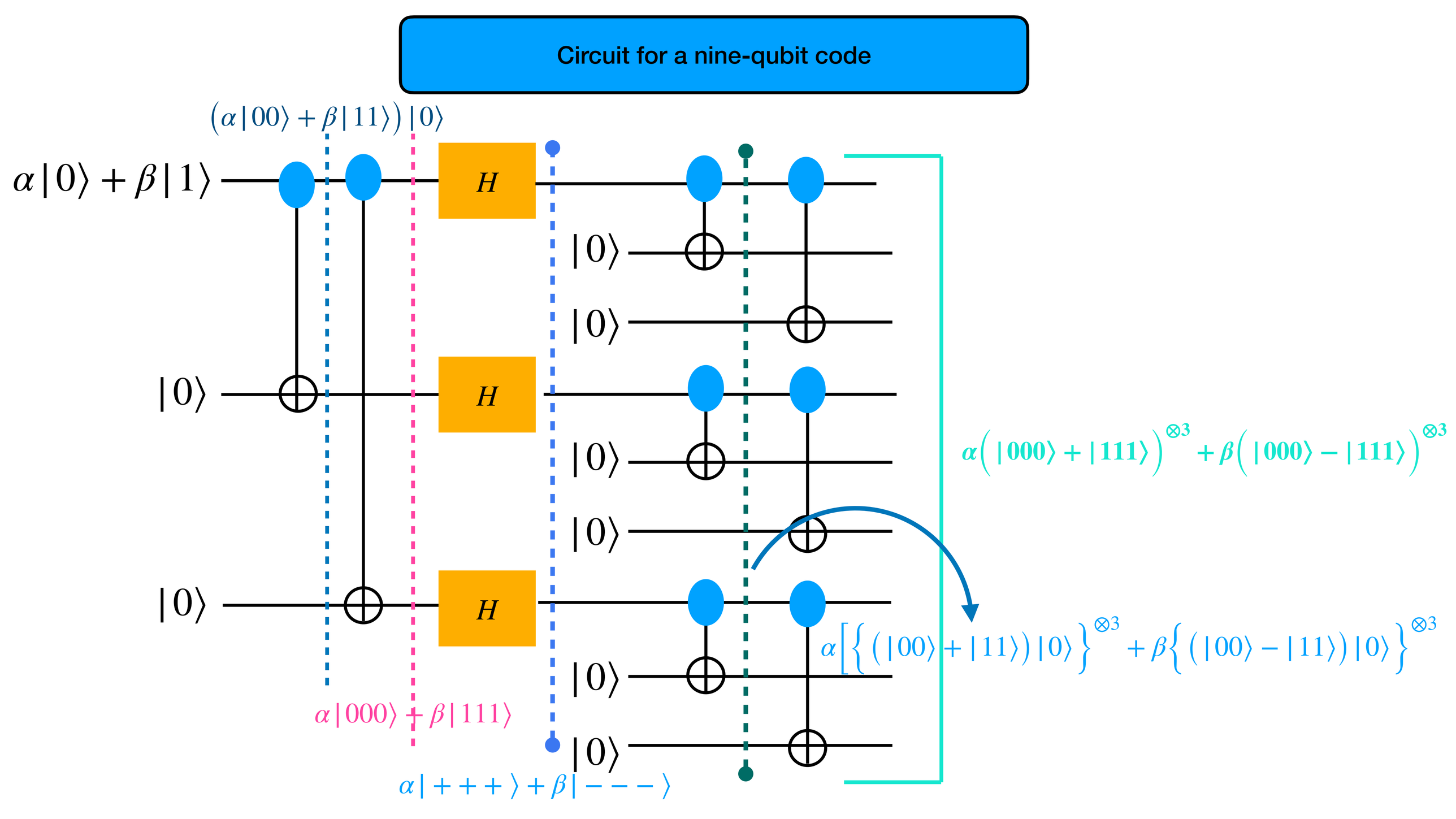


Circuit for a nine-qubit code



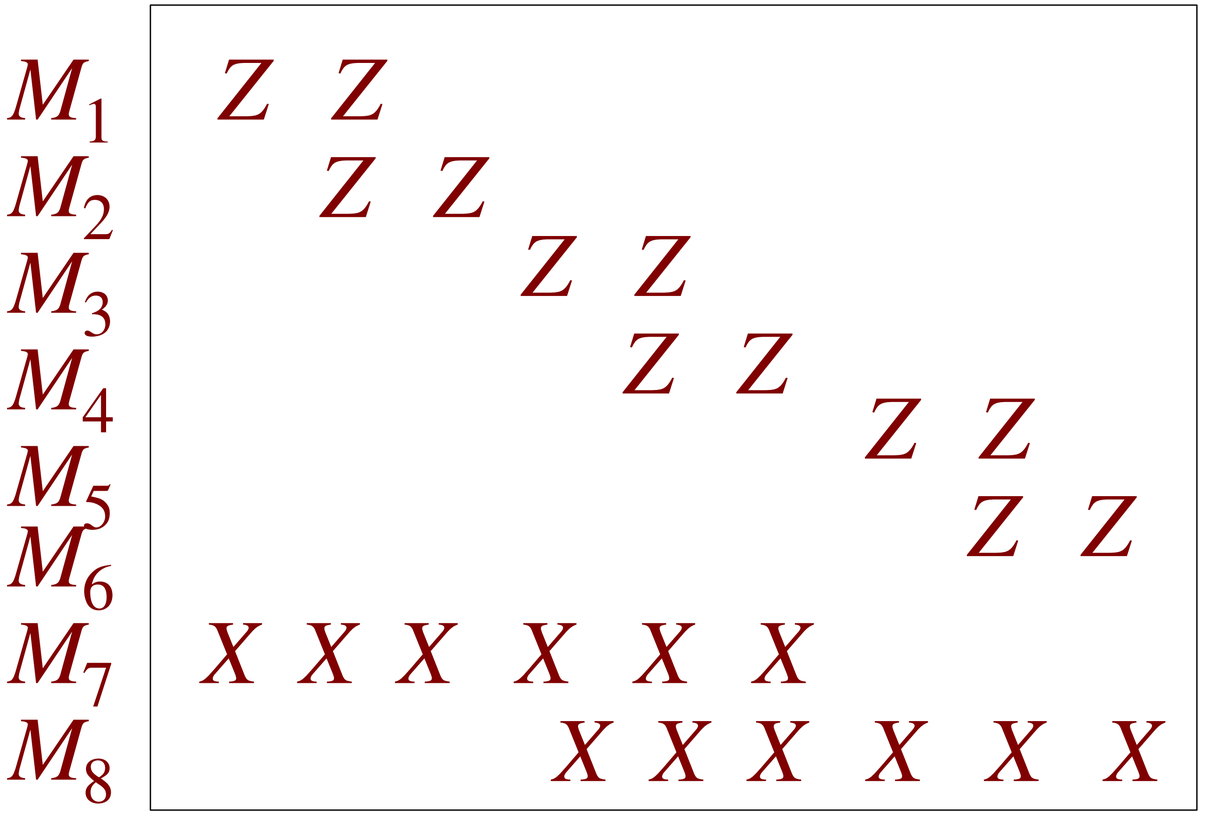
Circuit for a nine-qubit code




Circuit for a nine-qubit code
$(\alpha|00\rangle + \beta|11\rangle)|0\rangle$
$\alpha|0\rangle + \beta|1\rangle$
$|0\rangle$
$|0\rangle$
H
H
H
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$\alpha|000\rangle + \beta|111\rangle$
$\alpha|+++\rangle + \beta|---\rangle$
$\alpha\Big(|000\rangle + |111\rangle\Big)^{\otimes 3} + \beta\Big(|000\rangle - |111\rangle\Big)^{\otimes 3}$
$\alpha\Big[\Big\{(|00\rangle + |11\rangle)|0\rangle\Big\}^{\otimes 3} + \beta\Big\{(|00\rangle - |11\rangle)|0\rangle\Big\}^{\otimes 3}$

Stabilizer for Nine-Qubit Code

We can write down all the operators determining the syndrome for the nine-qubit code.



Update on the Problems

✓ 1. Measurement of error destroys superpositions.

✓ 2. No-cloning theorem prevents repetition.

✓ 3. Must correct multiple types of errors (e.g., bit flip and phase errors).

4. How can we correct continuous errors and decoherence?

Correcting Continuous Rotation

Let us rewrite continuous rotation

$$R_\theta|0\rangle = |0\rangle, R_\theta|1\rangle = e^{i\theta}|1\rangle$$

$$R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} = e^{i\theta/2}\begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix} = \cos\frac{\theta}{2} - i\sin\frac{\theta}{2}\sigma_z$$

$$R_\theta^{(k)}|\psi\rangle = \cos\frac{\theta}{2}|\psi\rangle - i\sin\frac{\theta}{2}Z^{(k)}|\psi\rangle$$

($R_\theta^{(k)}$ is R_θ acting on the k^{th} qubit.)

Correcting Continuous Rotations

How does error correction affect a state with a continuous rotation on it?

$$R_\theta^{(k)}|\psi\rangle = \cos\frac{\theta}{2}|\psi\rangle - i\sin\frac{\theta}{2}Z^{(k)}|\psi\rangle$$

$$\rightarrow \cos\frac{\theta}{2}|\psi\rangle|I\rangle - i\sin\frac{\theta}{2}Z^{(k)}|\psi\rangle|Z^{(k)}\rangle$$

Error syndrome

After measurement of error syndrome:

Prob. $\cos^2\frac{\theta}{2}$: $|\psi\rangle$ (no correction needed)

Prob. $\sin^2\frac{\theta}{2}$: $Z^{(k)}|\psi\rangle$ (corrected with $Z^{(k)}$)

Correcting All Single-Qubit Errors

Theorem: If a quantum error-correcting code (QECC) corrects errors A and B, it also corrects $\alpha A + \beta B$.

Any 2×2 matrix can be written as $\alpha I + \beta X + \gamma Y + \delta Z$.

A general single-qubit error $\rho \rightarrow \Sigma_k A_k \rho A_k^\dagger$ acts like a mixture of $|\psi\rangle \rightarrow A_k |\psi\rangle$, and A_k is a 2×2 matrix.

Any QECC that corrects the single-qubit errors X, Y, and Z (plus I) corrects every single-qubit error.

Correcting all t-qubit X, Y, Z on t qubits (plus I) corrects all t-qubit errors.

The Pauli Group (P_n)

Definition: Pauli group P_n on n qubits generated by $X, Y,$ and Z on individual qubits.

- P_n consists of all tensor products of up to n operators I, X, Y, Z with overall phase $\pm 1, \pm i$.

Any pair M, N of Pauli operators either commutes ($MN = NM$) or anticommutes ($MN = -NM$).

The weight of $M \in P_n$ is the number of qubits on which M acts as a non-identity operator.

The Pauli group spans the set of all n-qubit errors.

Small Error on Every Qubit

Suppose we have a small error U_ϵ on every qubit in the QECC, where $U_\epsilon = \mathbf{1} + \epsilon E$.

Then $U_\epsilon^{\otimes n} |\psi\rangle = |\psi\rangle + \epsilon(E^{(1)} + \cdots + E^{(n)})|\psi\rangle + o(\epsilon^2)$

If the code corrects one-qubit errors, it corrects the sum of the $E^{(i)}$. Therefore it corrects the $O(\epsilon)$ term, and the state remains correct to order ϵ^2.

A code correcting t errors keeps the state correct to order ϵ^{t+1}.

QECC is Possible

✓ 1. Measurement of error destroys superpositions.

✓ 2. No-cloning theorem prevents repetition.

✓ 3. Must correct multiple types of errors (e.g., bit flip and phase errors).

✓ 4. How can we correct continuous errors and decoherence?

PAUSE

QECC Conditions

Theorem.: A QECC can correct a set $\{E\}$ of errors iff

$$\langle \psi_i | E_a^\dagger E_b | \psi_j \rangle = C_{ab} \delta_{ij}$$

where the set $\{ |\psi_i\rangle \}$ forms a basis for the codewords, and $E_a, E_b \in E$.

Note: The matrix C_{ab} does not depend on i and j.

Example: $C_{ab} = \delta_{ab}$. Then we can make a measurement to determine the error.

Groups

A set $G = \{g\}$ is said to form a group under operation $*$ if the following properties are satisfied:

1. Closure: $\forall g_1, g_2 \in G, \quad g_1 * g_2 \in G\,.$

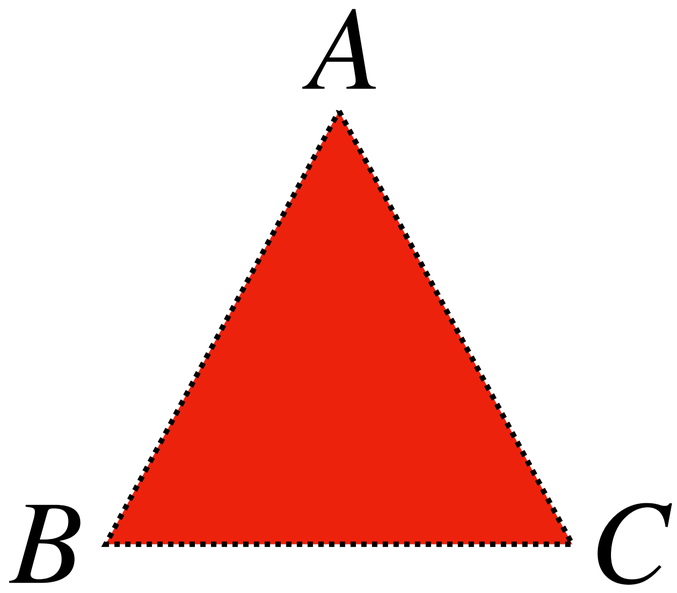
2. Existence of identity: There exists an element e such that $\forall g \in G, g * e = e * g = g\,.$

3. Existence of inverse: $\forall g \in G,$ there exists an element g^{-1} such that $g * g^{-1} = g^{-1} * g = e\,.$

4. Associativity: $\forall g_1, g_2, g_3 \in G, g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$

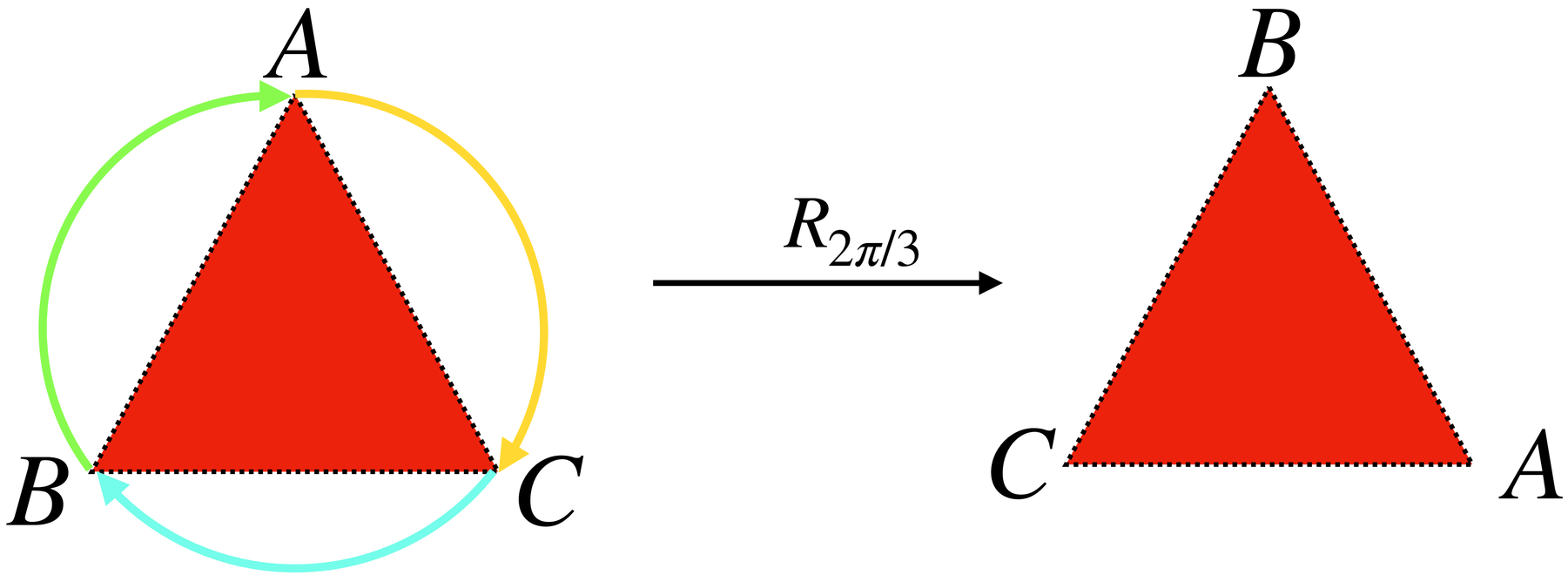
Tung, Wu-Ki. *Group theory in physics*. Vol. 1. World Scientific, 1985.

Example: Symmetry group of an equilateral triangle



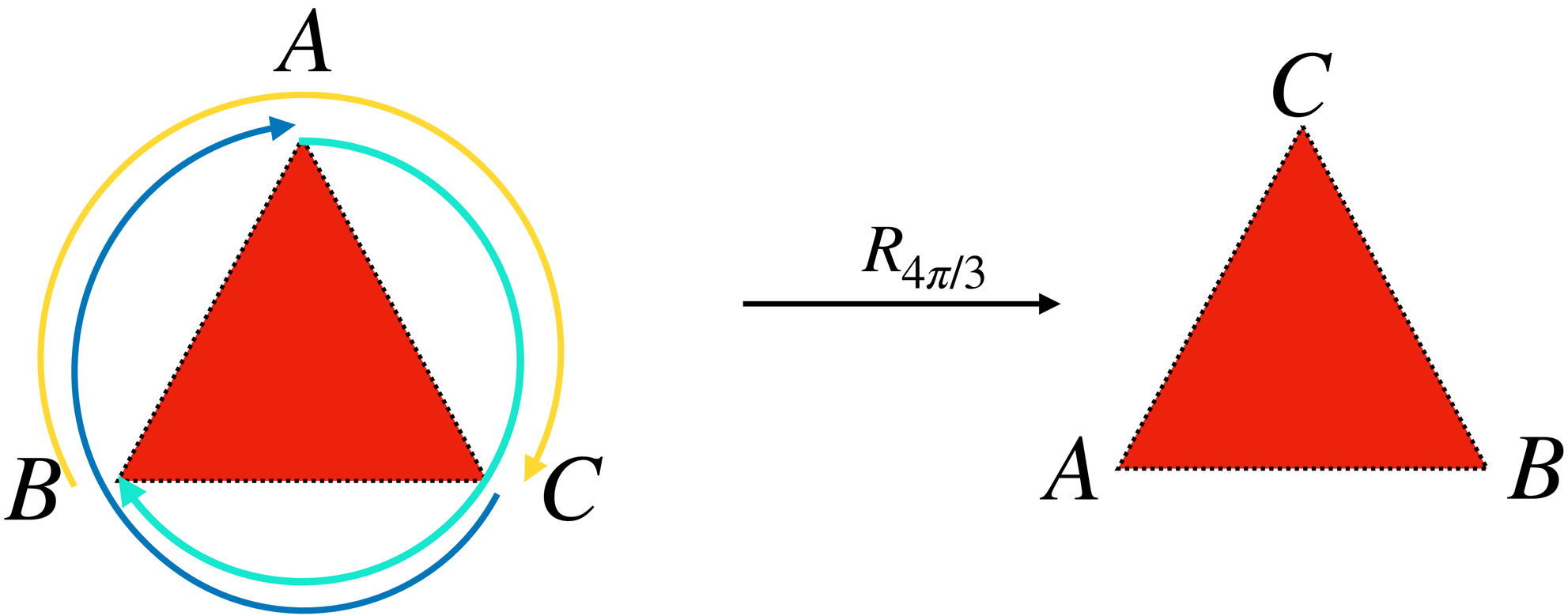
Tung, Wu-Ki. *Group theory in physics*. Vol. 1. World Scientific, 1985.

Example: Symmetry group of an equilateral triangle



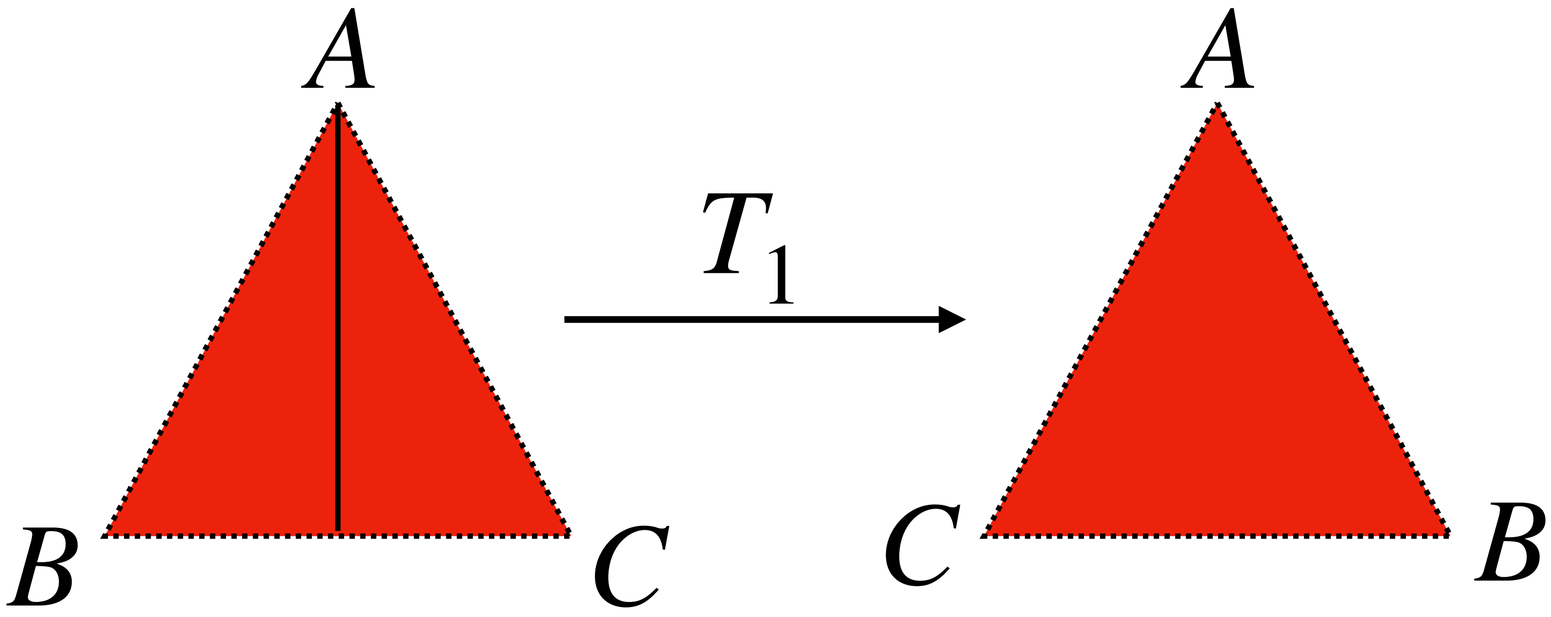
Tung, Wu-Ki. *Group theory in physics*. Vol. 1. World Scientific, 1985.

Example: Symmetry group of an equilateral triangle



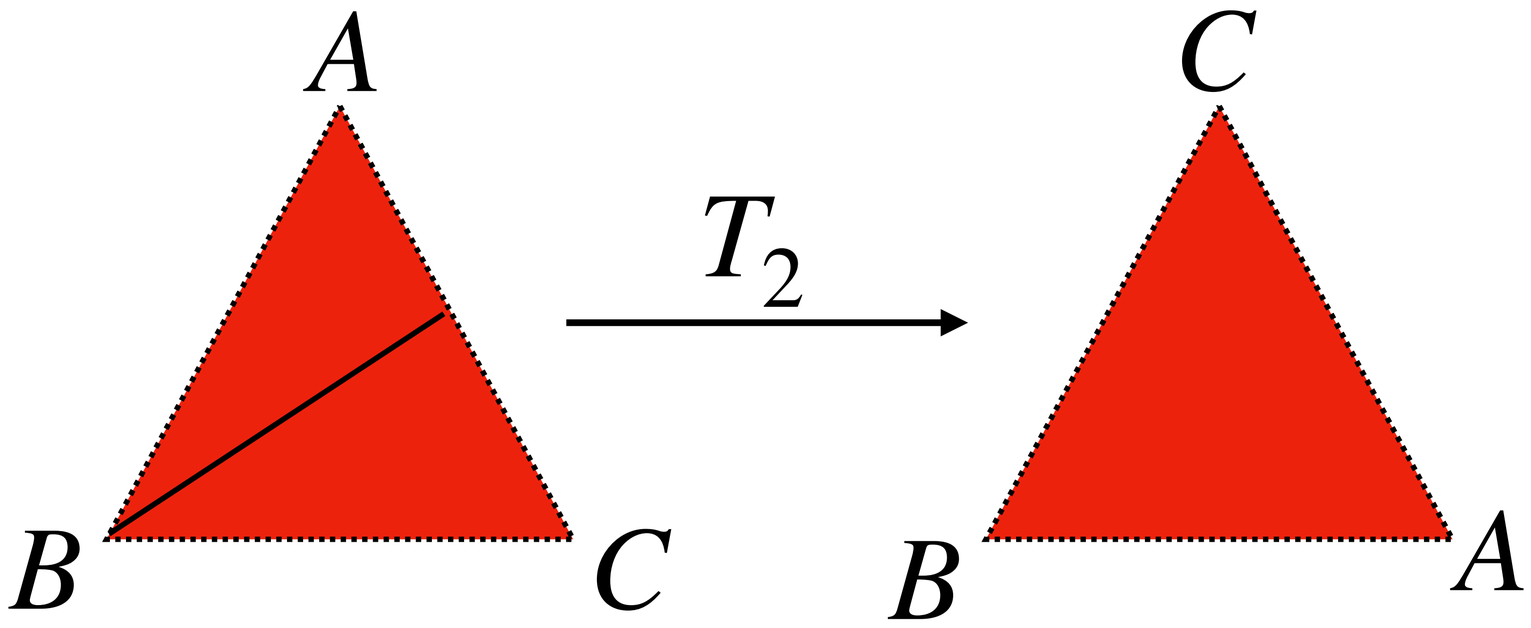
Tung, Wu-Ki. *Group theory in physics*. Vol. 1. World Scientific, 1985.

Example: Symmetry group of an equilateral triangle



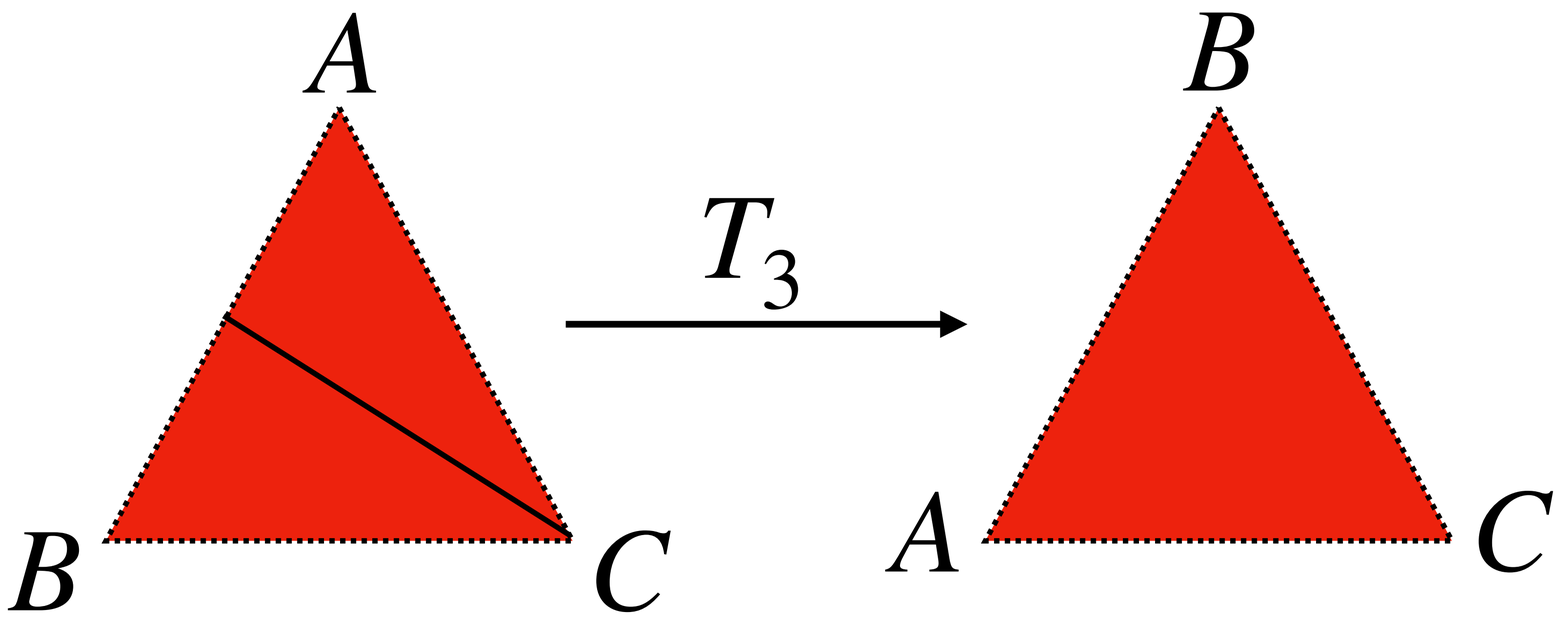
Tung, Wu-Ki. *Group theory in physics*. Vol. 1. World Scientific, 1985.

Example: Symmetry group of an equilateral triangle



Tung, Wu-Ki. *Group theory in physics*. Vol. 1. World Scientific, 1985.

Example: Symmetry group of an equilateral triangle



Tung, Wu-Ki. *Group theory in physics*. Vol. 1. World Scientific, 1985.

Symmetry group of an equilateral triangle: Group multiplication table

Exercise: Show this!

$*$	$\mathbf{1}$	$R_{2\pi/3}$	$R_{4\pi/3}$	T_1	T_2	T_3
$\mathbf{1}$	$\mathbf{1}$	$R_{2\pi/3}$	$R_{4\pi/3}$	T_1	T_2	T_3
$R_{2\pi/3}$	$R_{2\pi/3}$	$R_{4\pi/3}$	$\mathbf{1}$	T_2	T_3	T_1
$R_{4\pi/3}$	$R_{4\pi/3}$	$\mathbf{1}$	$R_{2\pi/3}$	T_3	T_1	T_2
T_1	T_1	T_3	T_2	$\mathbf{1}$	$R_{4\pi/3}$	$R_{2\pi/3}$
T_2	T_2	T_1	T_3	$R_{2\pi/3}$	$\mathbf{1}$	$R_{4\pi/3}$
T_3	T_3	T_2	T_1	$R_{4\pi/3}$	$R_{2\pi/3}$	$\mathbf{1}$

Stabiliser group

Stabilisers: Operators which have a state as their eigenstates with eigenvalue $+1$.

Example: $|\psi\rangle_L \equiv \frac{1}{\sqrt{2}}\Big(|0\rangle_L + |1\rangle_L \Big)$

$$\mathbf{1}_L |\psi\rangle_L = |\psi\rangle_L$$

$$X_L |\psi\rangle_L = |\psi\rangle_L$$

Stabiliser group

Stabilisers: Operators which have a state as their eigenstates with eigenvalue $+1$.

Example: $$|\psi\rangle_L \equiv \frac{1}{\sqrt{2}}\Big(|0\rangle_L + |1\rangle_L\Big)$$

$$\mathbf{1}_L|\psi\rangle_L = |\psi\rangle_L$$
$$X_L|\psi\rangle_L = |\psi\rangle_L$$

Instrumental in quantum error correction

*	$\mathbf{1}_L$	X_L
$\mathbf{1}_L$	$\mathbf{1}_L$	X_L
X_L	X_L	$\mathbf{1}_L$

Stabiliser group of a Bell state

$$|\psi\rangle_L \equiv \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big)$$

Stabiliser group of a Bell state

$$|\psi\rangle_L \equiv \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big)$$

$$\mathbf{1}_4 |\psi\rangle_L = |\psi\rangle_L$$

$$X_1 X_2 |\psi\rangle_L = |\psi\rangle_L$$

$$-Y_1 Y_2 |\psi\rangle_L = |\psi\rangle_L$$

$$Z_1 Z_2 |\psi\rangle_L = |\psi\rangle_L$$

Stabiliser group of a Bell state

$$|\psi\rangle_L \equiv \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big)$$

$$\mathbf{1}_4 |\psi\rangle_L = |\psi\rangle_L$$

$$X_1X_2 |\psi\rangle_L = |\psi\rangle_L$$

$$-Y_1Y_2 |\psi\rangle_L = |\psi\rangle_L$$

$$Z_1Z_2 |\psi\rangle_L = |\psi\rangle_L$$

$\bullet$	$\mathbf{1}_4$	X_1X_2	$-Y_1Y_2$	Z_1Z_2
$\mathbf{1}_4$	$\mathbf{1}_4$	X_1X_2	$-Y_1Y_2$	Z_1Z_2
X_1X_2	X_1X_2	$\mathbf{1}_4$	Z_1Z_2	$-Y_1Y_2$
$-Y_1Y_2$	$-Y_1Y_2$	Z_1Z_2	$\mathbf{1}_4$	X_1X_2
Z_1Z_2	Z_1Z_2	$-Y_1Y_2$	X_1X_2	$\mathbf{1}_4$

Stabilizer Codes

Error Syndromes Revisited

For correctly-encoded state 000 or 111: first two bits have even parity (an even number of 1's), and similarly for the 2nd and 3rd bits.

For state with error on one of the first two bits: odd parity for the first two bits.

A codeword is a +1 eigenvector of $Z \otimes Z \otimes I$ and a state with an error on the 1st or 2nd bit is a -1 eigenvector of $Z \otimes Z \otimes I$.

Error Syndromes Revisited

Three-qubit phase error correcting code:

Eigenvalue $+1$ for $X \otimes X \otimes \mathbf{1}$.

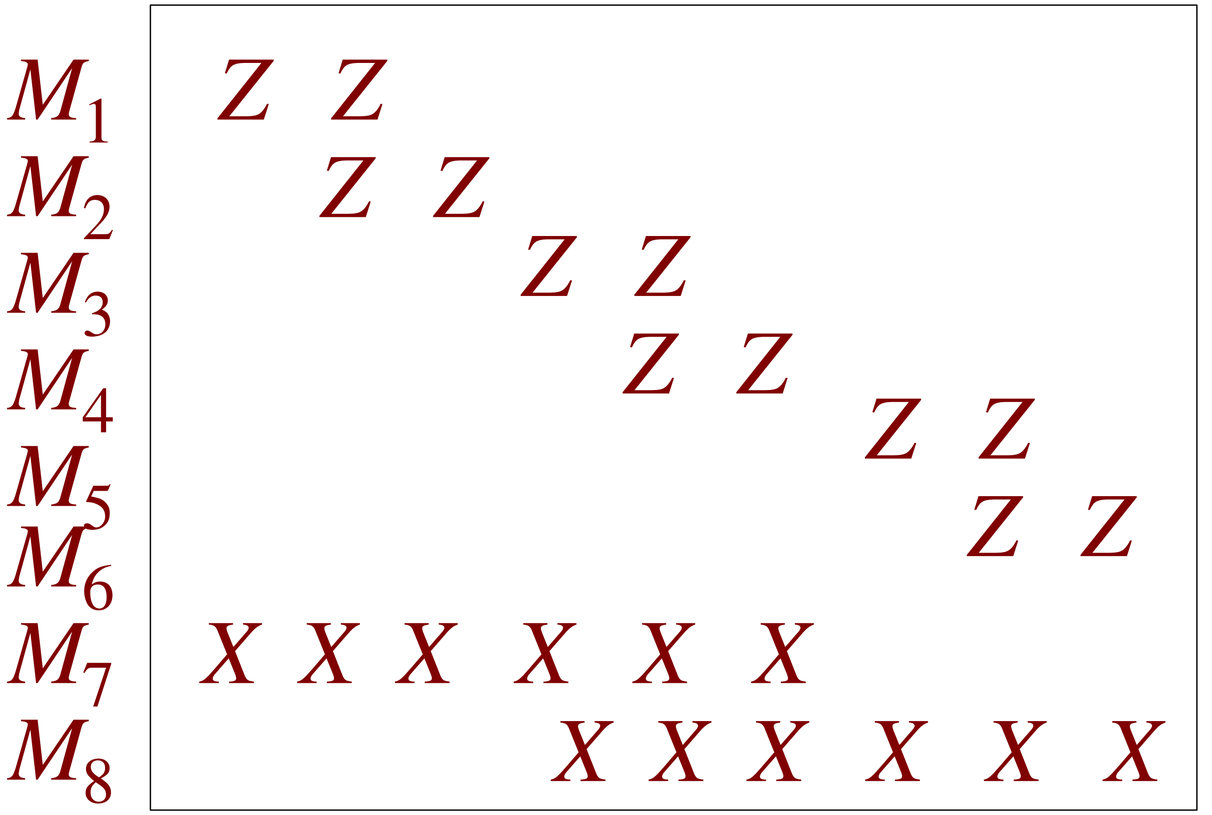
A state with a phase error on one of the first two qubits has eigenvalue -1 for $X \otimes X \otimes \mathbf{1}$.

Measuring $Z \otimes Z$ detects bit flip (X) errors, and measuring $X \otimes X$ detects phase (Z) errors.

Error syndrome is formed by measuring enough operators to determine location of error.

Stabilizer for Nine-Qubit Code

We can write down all the operators determining the syndrome for the nine-qubit code.



These generate a group, the stabilizer of the code, consisting of all Pauli operators M with the property that $M|\psi\rangle = |\psi\rangle$ for all encoded states $|\psi\rangle$.

Properties of a Stabilizer

The stabilizer is a group:

If $M|\psi\rangle = |\psi\rangle$ and $N|\psi\rangle = |\psi\rangle$, then $MN|\psi\rangle = |\psi\rangle$.

The stabilizer is Abelian:

If $M|\psi\rangle = |\psi\rangle$ and $N|\psi\rangle = |\psi\rangle$, then

$$(MN - NM)|\psi\rangle = 0$$

(For Pauli matrices)  $MN = NM$

Given any Abelian group S of Pauli operators, define a code space
$T(S) = \{|\psi\rangle \text{ s.t. } M|\psi\rangle = |\psi\rangle \forall M \in S\}$.

Then $T(S)$ encodes k logical qubits in n physical qubits when S has $n-k$ generators (so size 2^{n-k}).

Stabilizer Elements Detect Errors

Suppose $M \in S$ and Pauli error E anticommutes with M. Then:

$$M\,(E\,|\,\psi\rangle\,) = -\,EM\,|\,\psi\rangle\; = -\,E\,|\,\psi\rangle\;,$$

so $E\,|\,\psi\rangle$ has eigenvalue -1 for M.

Conversely, if M and E commute for all $M \in S$,

$$M\,(E\,|\,\psi\rangle\,) = EM\,|\,\psi\rangle\; = E\,|\,\psi\rangle\qquad \forall\, M \in S,$$

so $E\,|\,\psi\rangle$ has eigenvalue +1 for all M in the stabilizer.

The eigenvalue of an operator M from the stabilizer detects errors which anticommute with M.

Distance of a Stabilizer Code

Let S be a stabilizer, and let T(S) be the corresponding QECC. Define

$$N(S) = \{N \in P_n \text{ s.t. } MN=NM \ \forall \ M \in S\}.$$

Then the distance d of T(S) is the weight of the smallest Pauli operator N in N(S) \ S.

The code detects any error not in N(S) \ S (i.e., errors which commute with the stabilizer are not detected).

Why minus S? “Errors” in S leave all codewords fixed, so are not really errors. (Degenerate QECC.)

Error Syndromes and Stabilizers

To correct errors, we must accumulate enough information about the error to figure out which one occurred.

The error syndrome is the list of eigenvalues of the generators of S: If the error E commutes with $M \in S$, then M has eigenvalue +1; if E and M anticommute, M has eigenvalue -1.

We can then correct a set of possible errors if they all have distinct error syndromes.

Application: 5-Qubit Code

We can generate good codes by picking an appropriate stabilizer. For instance:

$$X \otimes Z \otimes Z \otimes X \otimes \mathbf{1}$$
$$\mathbf{1} \otimes X \otimes Z \otimes Z \otimes X$$
$$X \otimes \mathbf{1} \otimes X \otimes Z \otimes Z$$
$$Z \otimes X \otimes \mathbf{1} \otimes X \otimes Z$$

$n = 5$ physical qubits

-4 generators of S

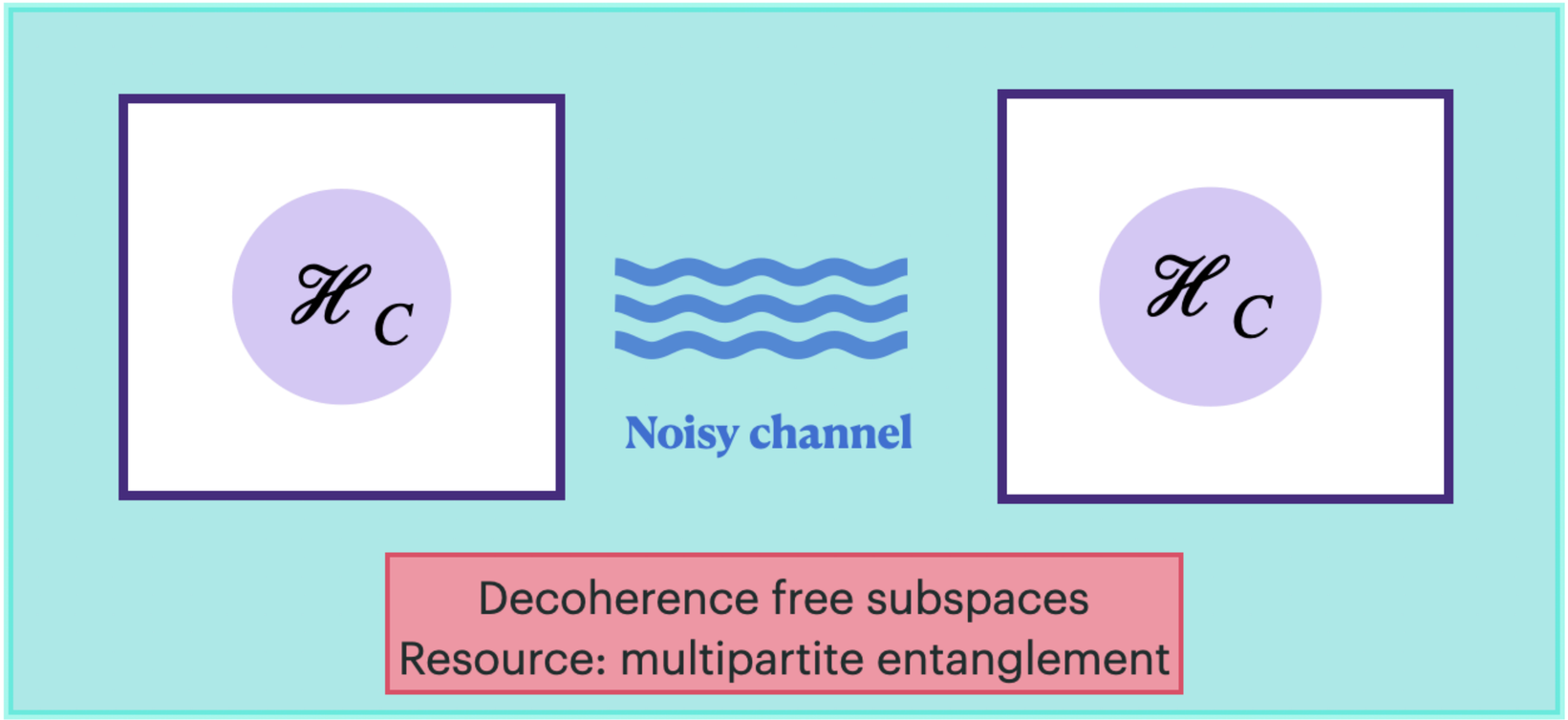
$k = 1$ encoded qubit

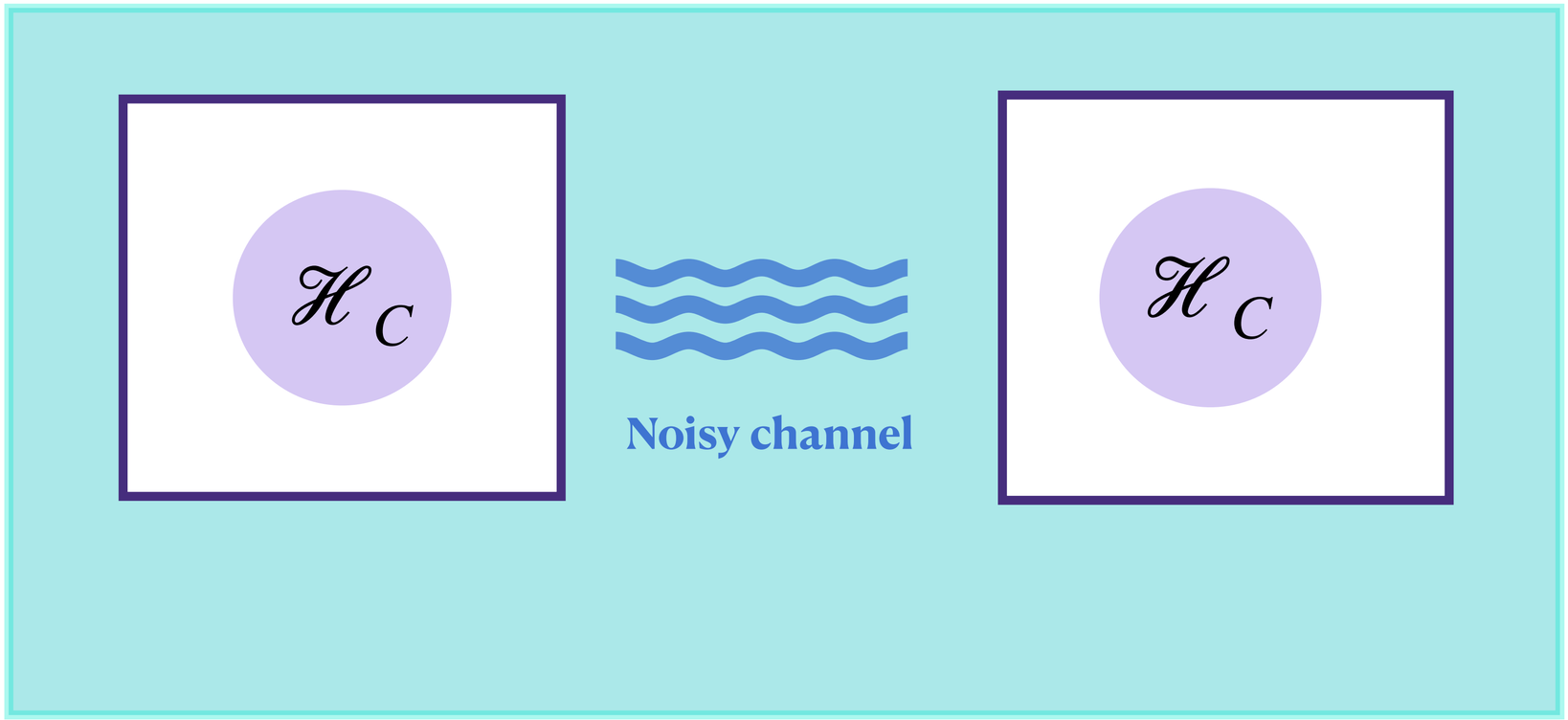
Distance d of this code is 3.

Notation: [[n,k,d]] for a QECC encoding k logical qubits in n physical qubits with distance d.
The five-qubit code is a non-degenerate [[5,1,3]] QECC.

PAUSE

Other error correction techniques


$\mathcal{H}_C$
Noisy channel
$\mathcal{H}_C$
Decoherence free subspaces
Resource: multipartite entanglement



Example: $|00\rangle + |11\rangle \xrightarrow{Z_1 Z_2} |00\rangle + |11\rangle$

$Z|0\rangle = |0\rangle$

$Z|1\rangle = -|1\rangle$

- Decoherence free subspaces: subspaces that remain invariant under noisy evolution.

$$\alpha|00\rangle + \beta|11\rangle \xrightarrow{Z_1 Z_2} \alpha|00\rangle + \beta|11\rangle$$

$$Z|0\rangle = |0\rangle$$
$$Z|1\rangle = -|1\rangle$$

- Quantum error rejecting codes: detects whether error has occurred or not.

Example: single bit-flip

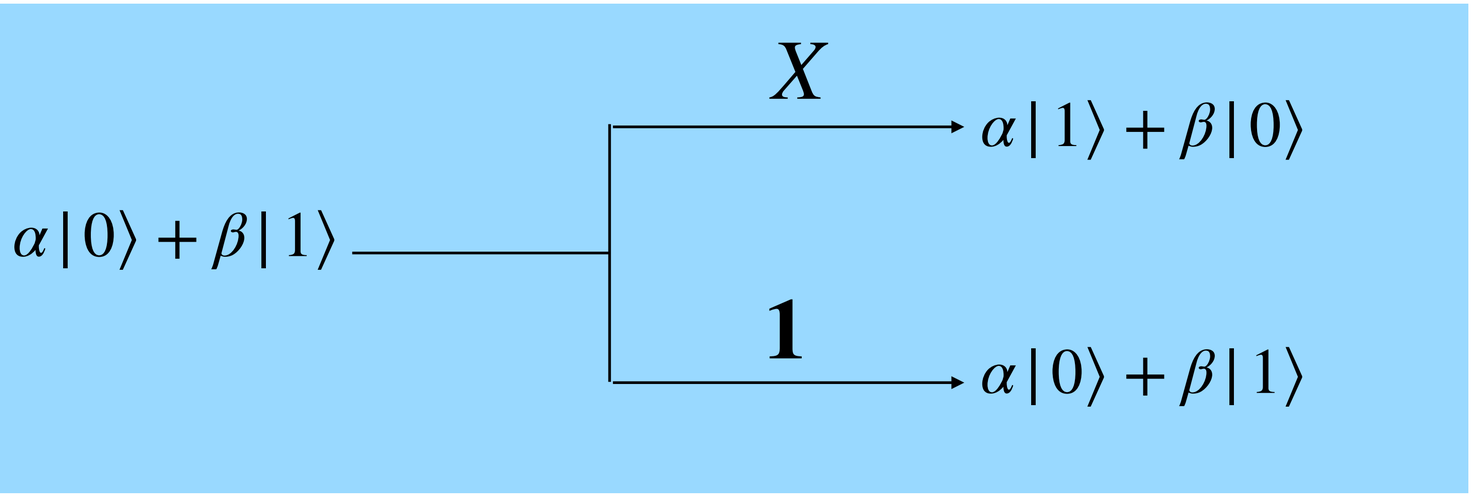
$\{\sqrt{p}, X_i\}$

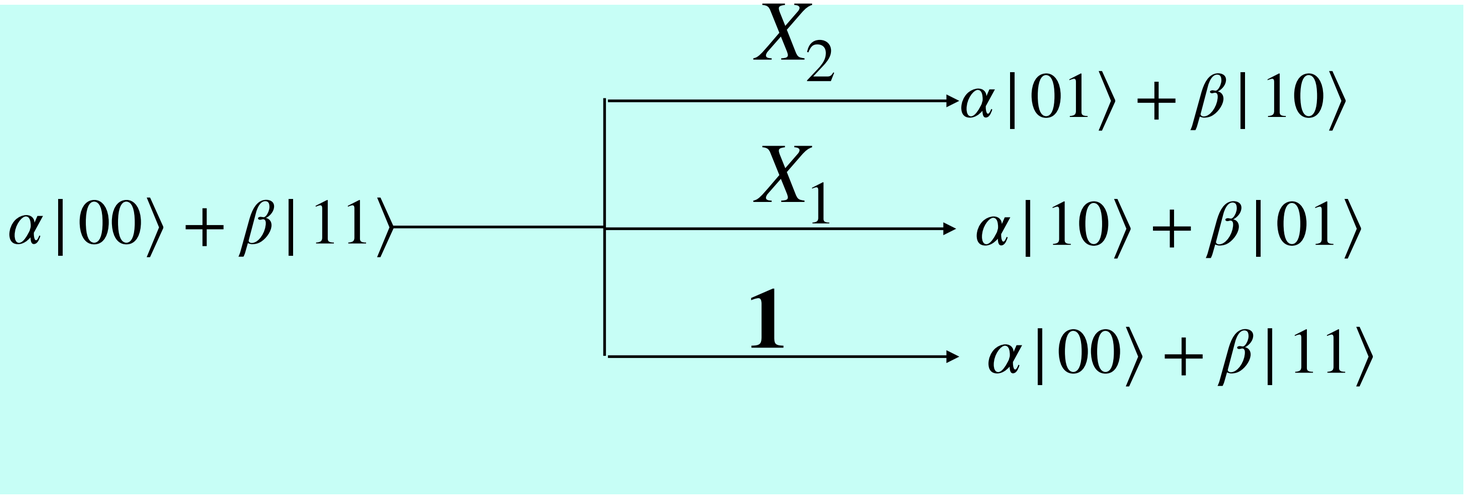
Resource state $\alpha|00\rangle + \beta|11\rangle$

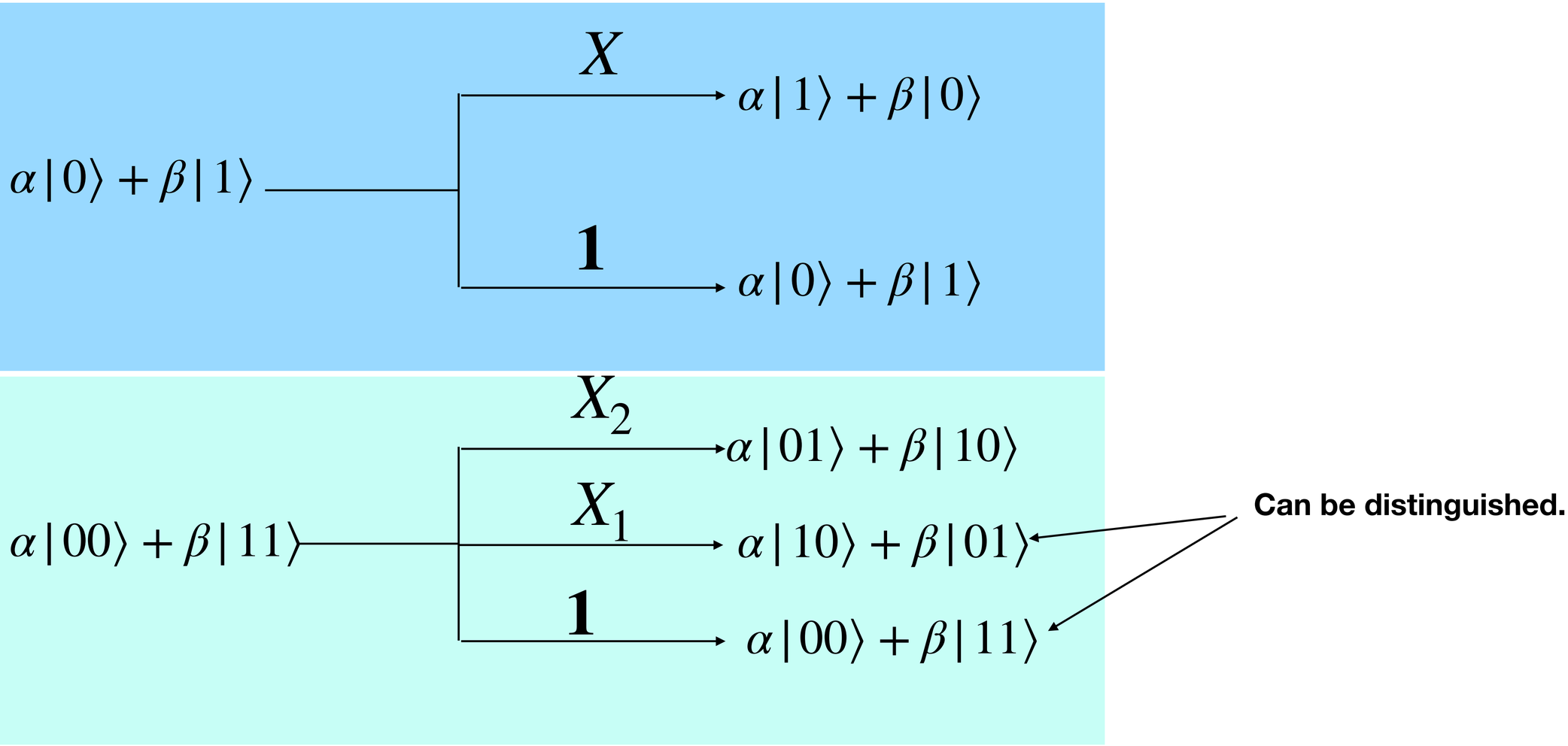
$Z_1 Z_2$

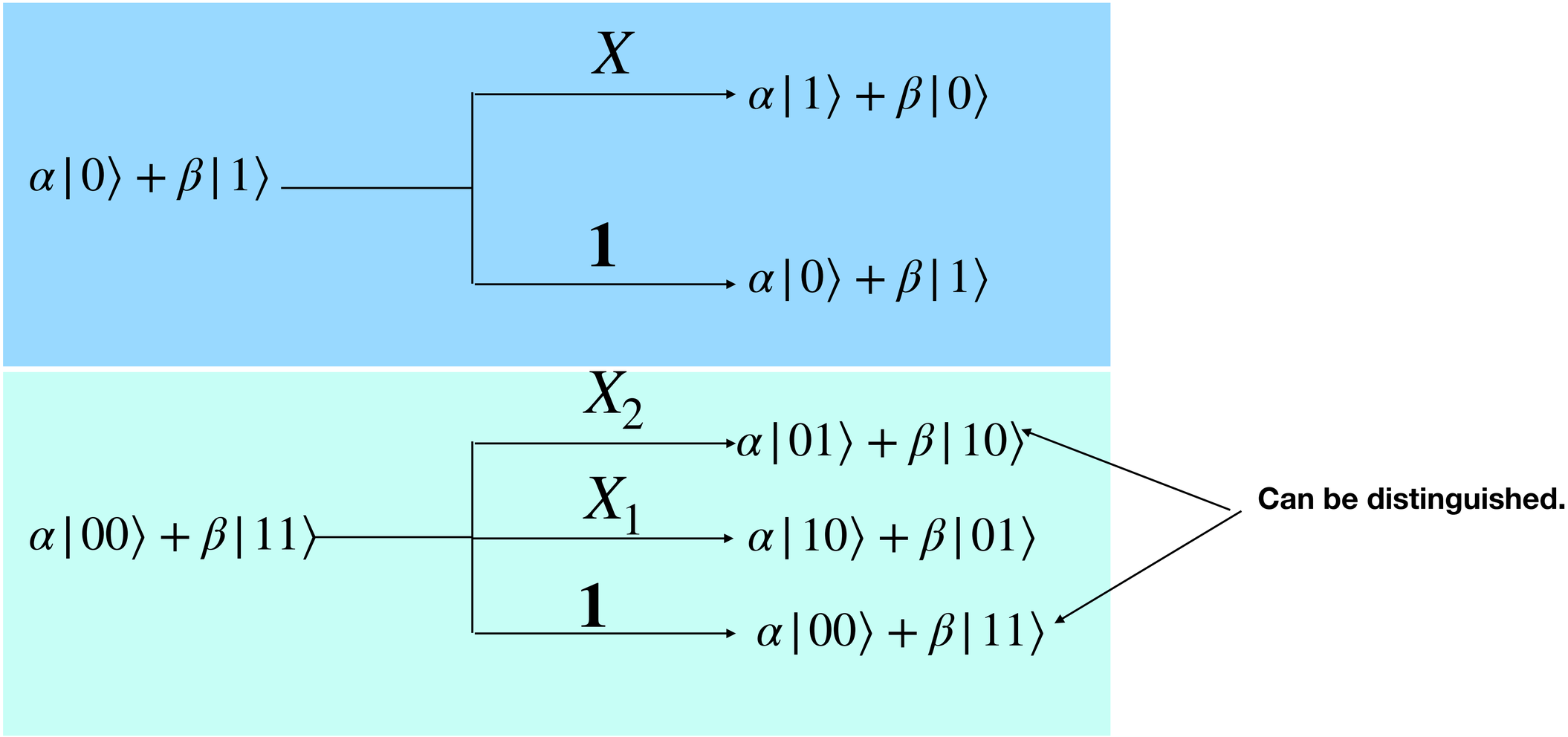
$\alpha|01\rangle + \beta|10\rangle$

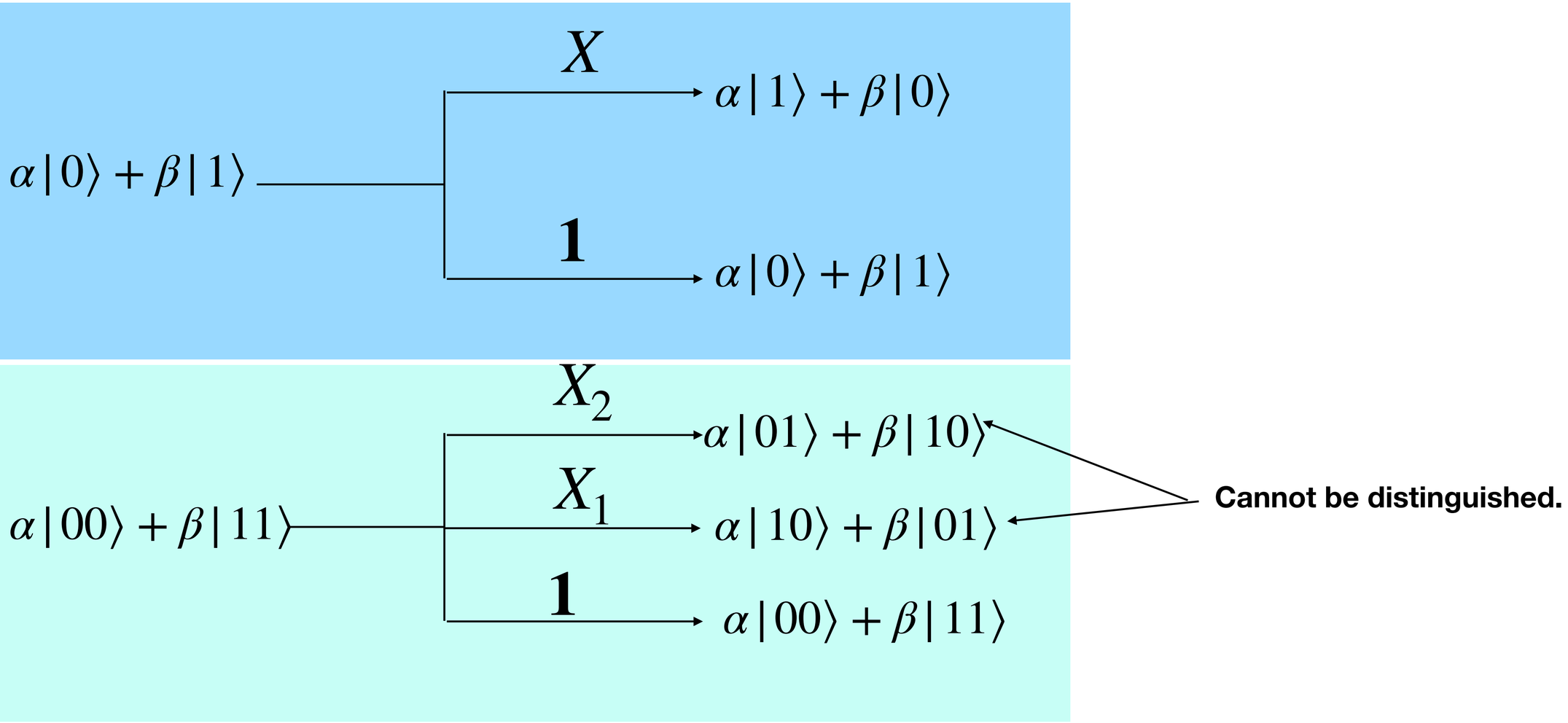
$\alpha|10\rangle + \beta|01\rangle$


X
$\alpha|1\rangle + \beta|0\rangle$
$\alpha|0\rangle + \beta|1\rangle$
$\mathbf{1}$
$\alpha|0\rangle + \beta|1\rangle$


X_2
$\alpha|01\rangle + \beta|10\rangle$
X_1
$\alpha|00\rangle + \beta|11\rangle$
$\alpha|10\rangle + \beta|01\rangle$
$\mathbf{1}$
$\alpha|00\rangle + \beta|11\rangle$


X
$\alpha|1\rangle + \beta|0\rangle$
$\alpha|0\rangle + \beta|1\rangle$
$\mathbf{1}$
$\alpha|0\rangle + \beta|1\rangle$
X_2
$\alpha|01\rangle + \beta|10\rangle$
X_1
$\alpha|10\rangle + \beta|01\rangle$
$\alpha|00\rangle + \beta|11\rangle$
$\mathbf{1}$
$\alpha|00\rangle + \beta|11\rangle$
Can be distinguished.


X
$\alpha|1\rangle + \beta|0\rangle$
$\alpha|0\rangle + \beta|1\rangle$
$\mathbf{1}$
$\alpha|0\rangle + \beta|1\rangle$
X_2
$\alpha|01\rangle + \beta|10\rangle$
X_1
$\alpha|10\rangle + \beta|01\rangle$
$\alpha|00\rangle + \beta|11\rangle$
$\mathbf{1}$
$\alpha|00\rangle + \beta|11\rangle$
Can be distinguished.


X
$\alpha|1\rangle + \beta|0\rangle$
$\alpha|0\rangle + \beta|1\rangle$
$\mathbf{1}$
$\alpha|0\rangle + \beta|1\rangle$
X_2
$\alpha|01\rangle + \beta|10\rangle$
X_1
$\alpha|10\rangle + \beta|01\rangle$
$\alpha|00\rangle + \beta|11\rangle$
$\mathbf{1}$
$\alpha|00\rangle + \beta|11\rangle$
Cannot be distinguished.

What about CV systems?

Gottesman-Kitaev-Preskill (GKP) codes

-Working around the uncertainty principle

Heisenberg uncertainty principle :
position and momentum cannot be measured simultaneously

$$[\hat{q}, \hat{p}] = i \neq 0$$

BUT, can be measured simultaneously in modulo √π

$[\hat{S}_q, \hat{S}_p] = 0$ where

$$\hat{S}_q = e^{i2\sqrt{\pi}\hat{q}} = \hat{D}(i\sqrt{2\pi})$$

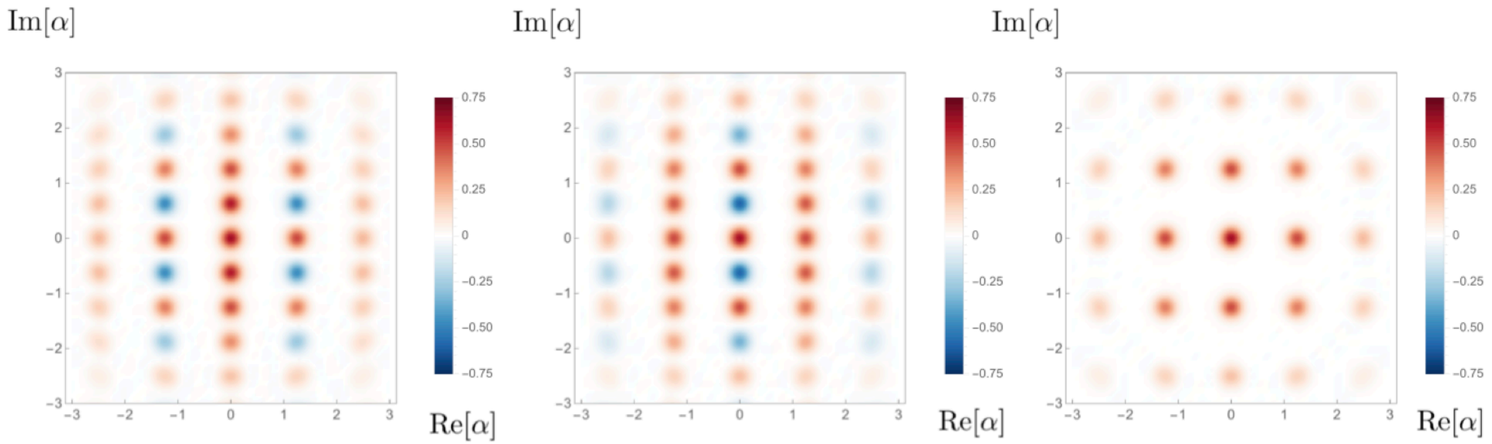
$$\hat{S}_p = e^{-i2\sqrt{\pi}\hat{q}} = \hat{D}(\sqrt{2\pi})$$

: stabilizers of the (square lattice) GKP code

D. Gottesman, A. Kitaev, and J. Preskill, Phys. Rev. A **64**, 012310 (2001)

Logical states of the (square-lattice) GKP code

-Wigner function of the logical states



Logical 0 Logical 1 Maximally mixed

$$|0_L\rangle \propto \sum_{n\in\mathbb{Z}} |\hat{q} = (2n)\sqrt{\pi}\rangle \qquad |+_L\rangle \propto |0_L\rangle + |1_L\rangle \propto \sum_{n\in\mathbb{Z}} |\hat{p} = (2n)\sqrt{\pi}\rangle$$

$$|1_L\rangle \propto \sum_{n\in\mathbb{Z}} |\hat{q} = (2n+1)\sqrt{\pi}\rangle \qquad |-_L\rangle \propto |0_L\rangle - |1_L\rangle \propto \sum_{n\in\mathbb{Z}} |\hat{p} = (2n-1)\sqrt{\pi}\rangle$$

$$\Rightarrow \hat{q} = \hat{p} \equiv 0 \mod \sqrt{\pi}$$

Gaussian random displacement channel

-Definition

$$\mathcal{N}_{B_2}[\sigma^2](\hat{\rho}) = \frac{1}{\pi\sigma^2}\int d^2\alpha e^{-\frac{|\alpha|^2}{\sigma^2}}\hat{D}(\alpha)\hat{\rho}\hat{D}^{\dagger}(\alpha)$$

σ^2 : variance of random displacement

$\Delta_q = \sqrt{2}\mathrm{Re}[\alpha]$: random displacement in the position quadrature

$\Delta_p = \sqrt{2}\mathrm{Im}[\alpha]$: random displacement in the momentum quadrature

-Decoding the square lattice GKP code

measure $\hat{q}$ and $\hat{p}$ in modulo $\sqrt{\pi}$

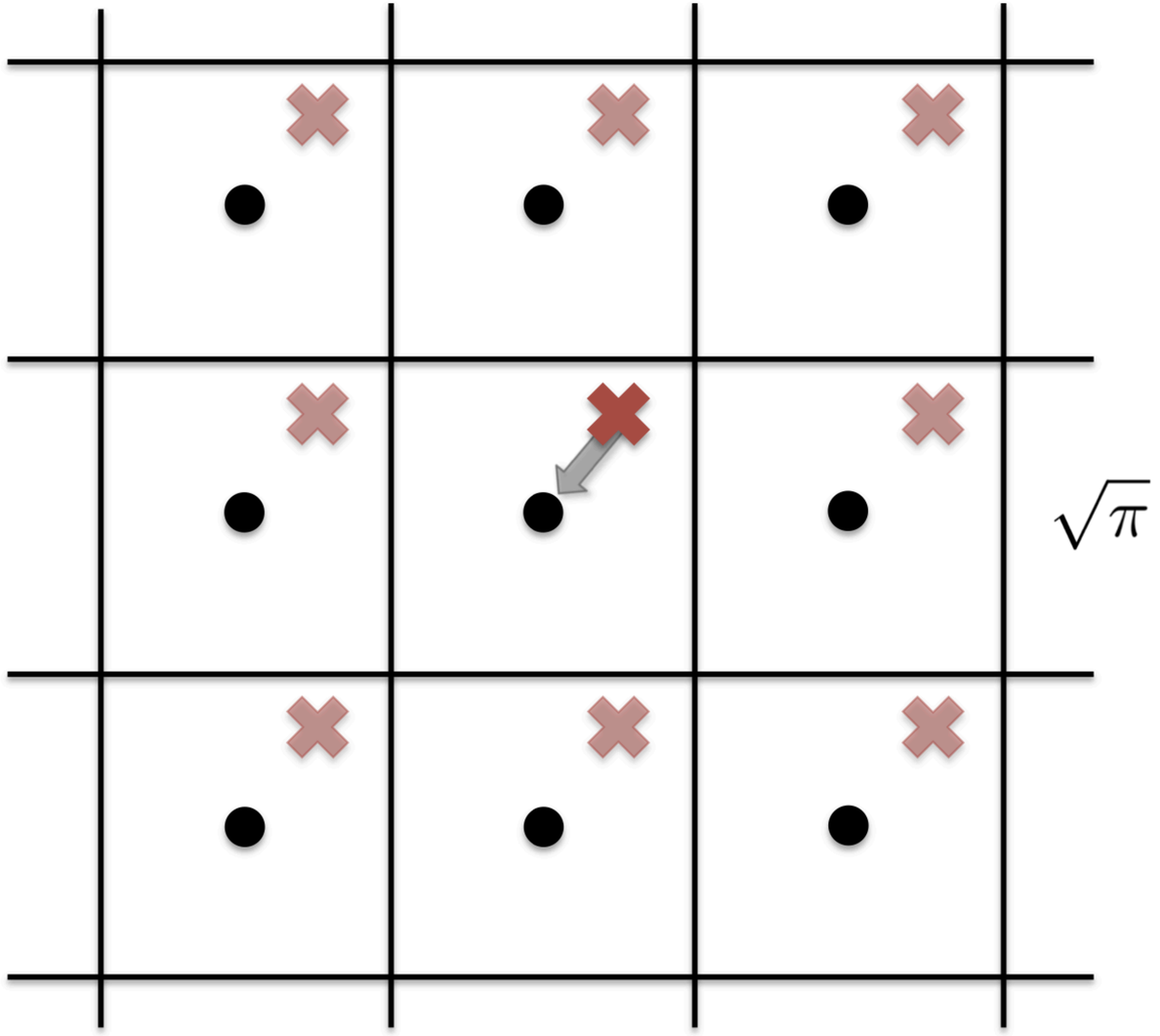
➡ $\Delta_q = \Delta_q^{\star} + n_q\sqrt{\pi}$ and $\Delta_p = \Delta_p^{\star} + n_p\sqrt{\pi}$

where $\Delta_q^{\star}, \Delta_p^{\star} \in (-\frac{\sqrt{\pi}}{2}, \frac{\sqrt{\pi}}{2}]$

➡ infer $\Delta_q = \Delta_q^{\star}$ and $\Delta_p = \Delta_p^{\star}$, then implement the counter displacement

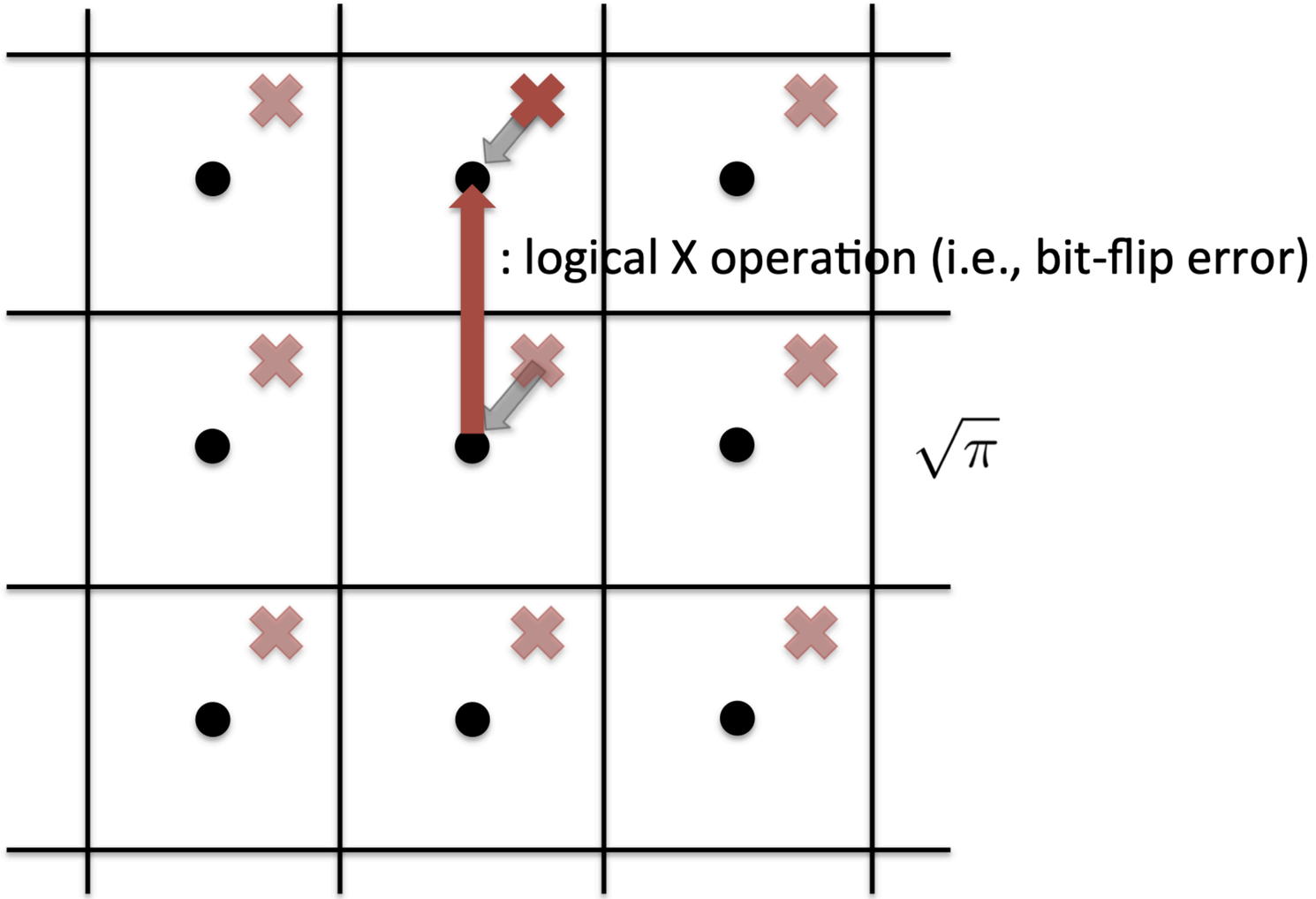
Conventional GKP decoding

-Successful decoding



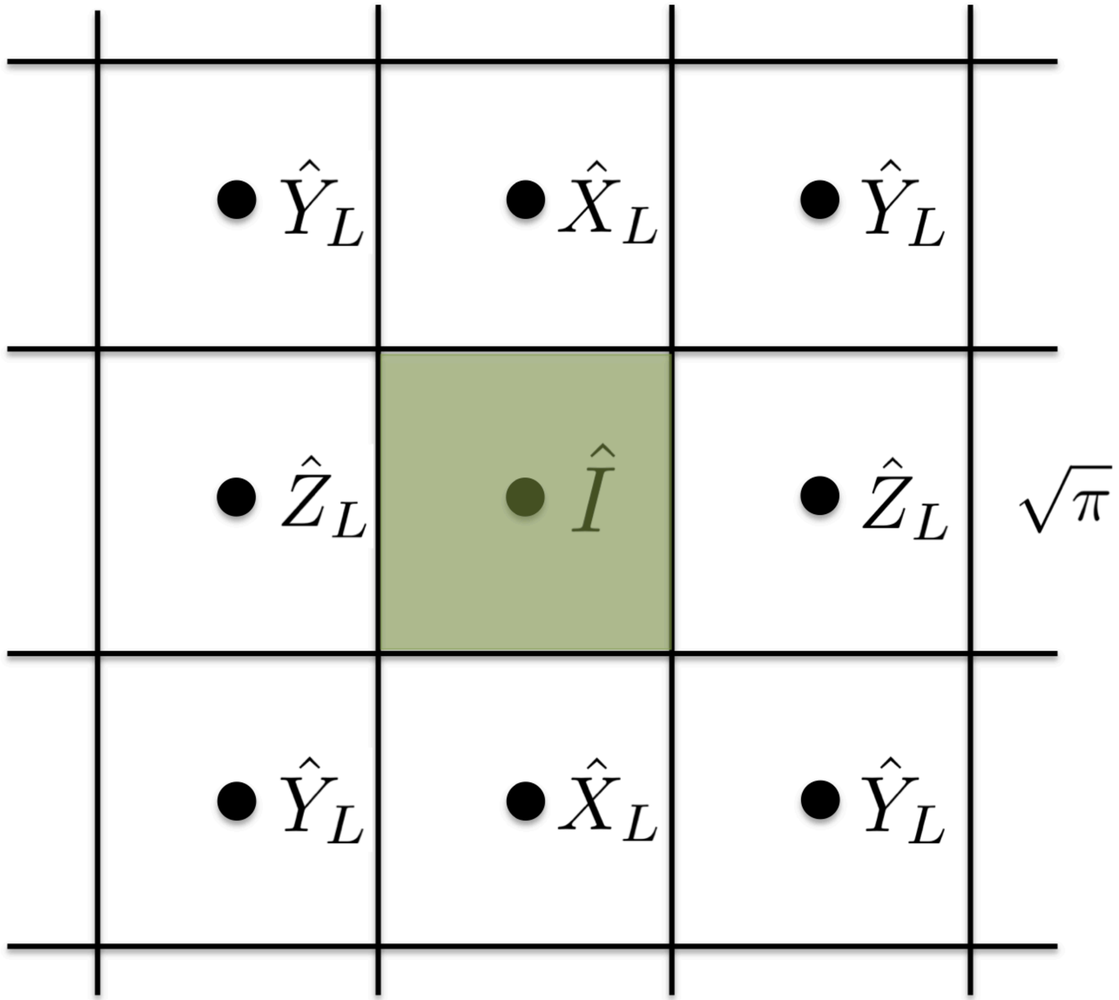
Conventional GKP decoding

-Failed decoding



Conventional GKP decoding

-Failed decoding



Success probability

$$
\begin{aligned}
P_{\mathrm{succ}} &= \frac{1}{2\pi\sigma^2} \int_{-\frac{\sqrt{\pi}}{2}}^{\frac{\sqrt{\pi}}{2}} d\Delta_q \int_{-\frac{\sqrt{\pi}}{2}}^{\frac{\sqrt{\pi}}{2}} d\Delta_p e^{-\frac{\Delta_q^2+\Delta_p^2}{2\sigma^2}} \\
&\geq \frac{1}{2\pi\sigma^2} \int_0^{\frac{\sqrt{\pi}}{2}} r dr \int_0^{2\pi} d\theta e^{-\frac{r^2}{2\sigma^2}} \\
&= \int_0^{\frac{\pi}{8\sigma^2}} dx e^{-x} \\
&= 1 - \exp\left[-\frac{\pi}{8\sigma^2} \right]
\end{aligned}
$$

Conclusions

- Error correction codes are possible to construct.
- Entanglement acts as a resource in them.
- Overhead of resources.

Is this the end of the story?

- Of course not. In fact, the low efficiency of entangling gates poses a challenge.
- Calls for alternate resource friendly solutions.

Quantum Errors

A general quantum error is a superoperator.

$$\rho \to \sum_k A_k \rho A_k^\dagger$$

Examples:

Bit Flip X: $X|0\rangle = |1\rangle, \;\; X|1\rangle = |0\rangle$

Phase Flip Z: $Z|0\rangle = |0\rangle, \;\; Z|1\rangle = -|1\rangle$

Rotation: $R_\theta|0\rangle = |0\rangle, \; R_\theta|1\rangle = e^{i\theta}|1\rangle$

Tutorial