Sharif Quantum Information Group

An introduction to Quantum Error Correction-I

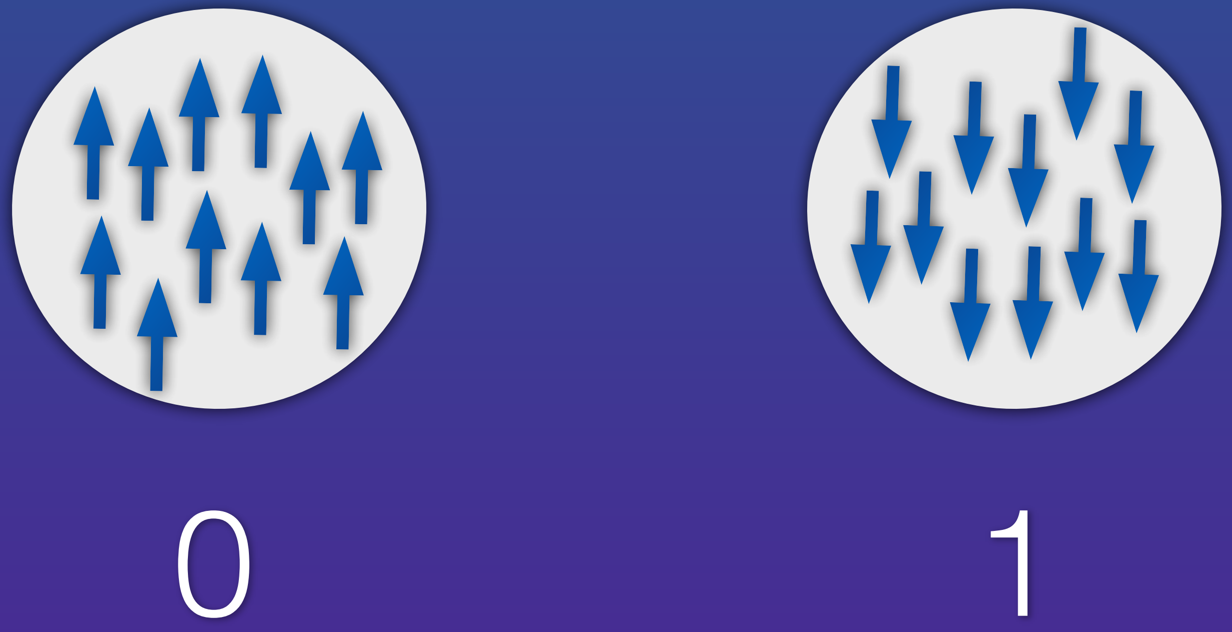
Vahid Karimipour,
Sharif University of Technology, Iran.

School on Quantum Information and Holography

Classical Bits

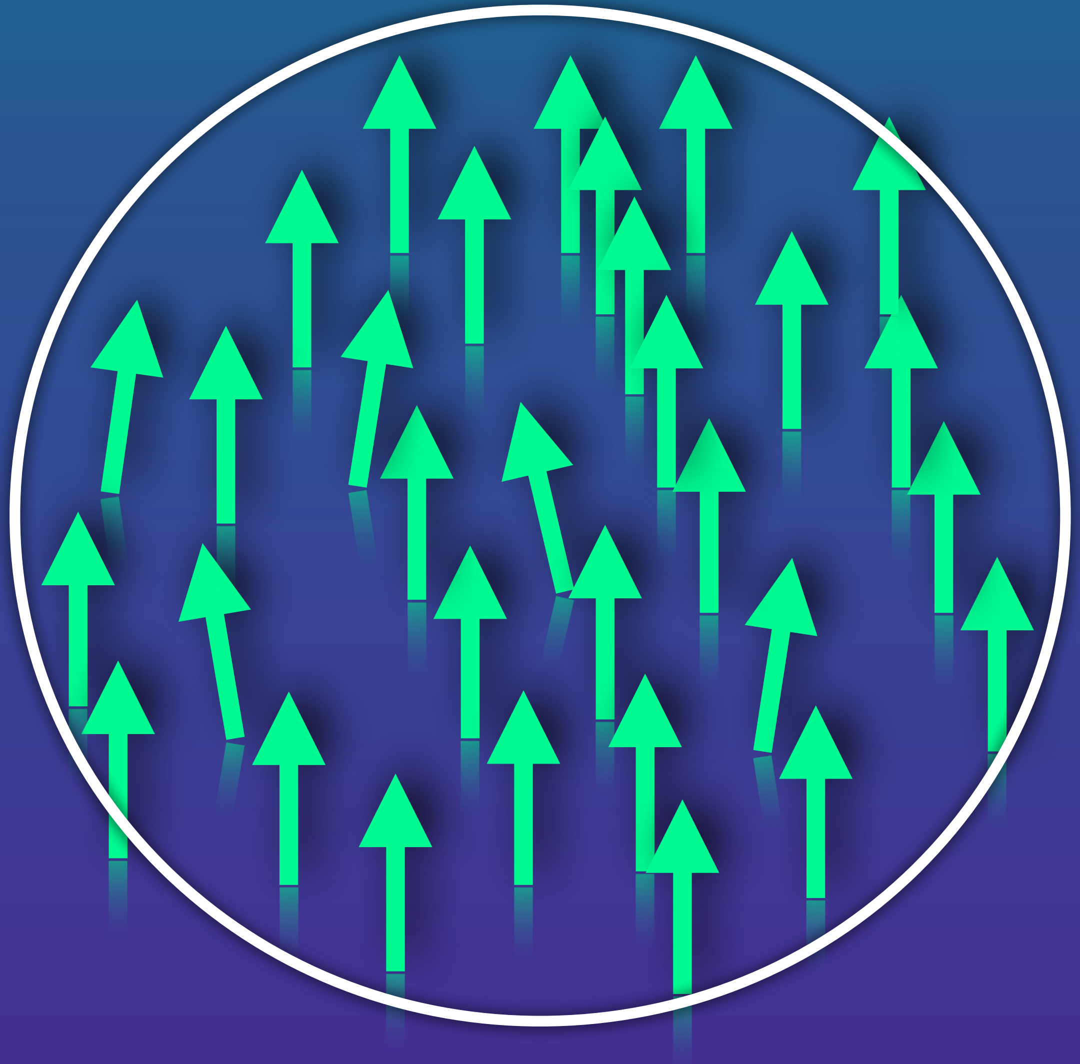
Have four basic properties.

1- Bits are Macroscopic Objects

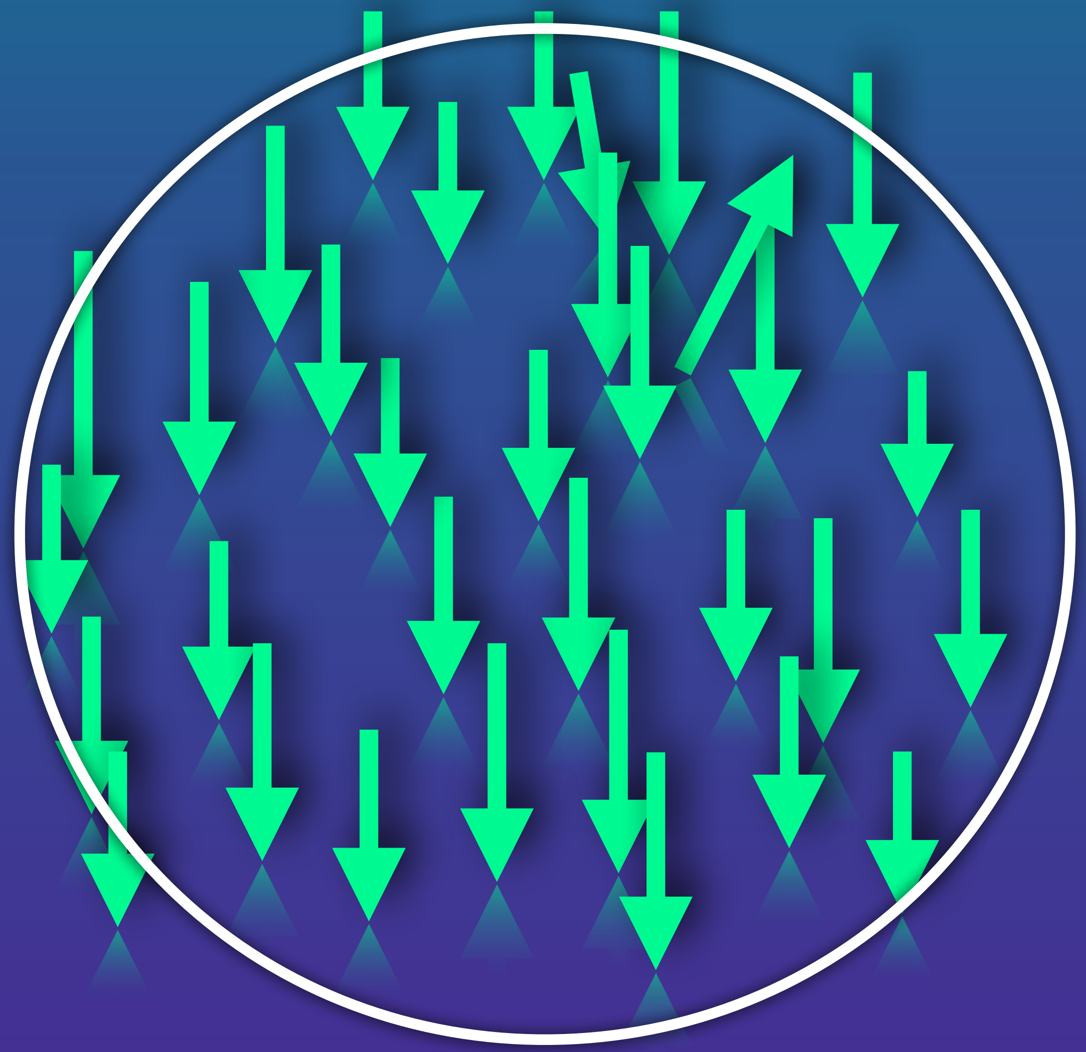


So classical bits are almost very robust against errors.

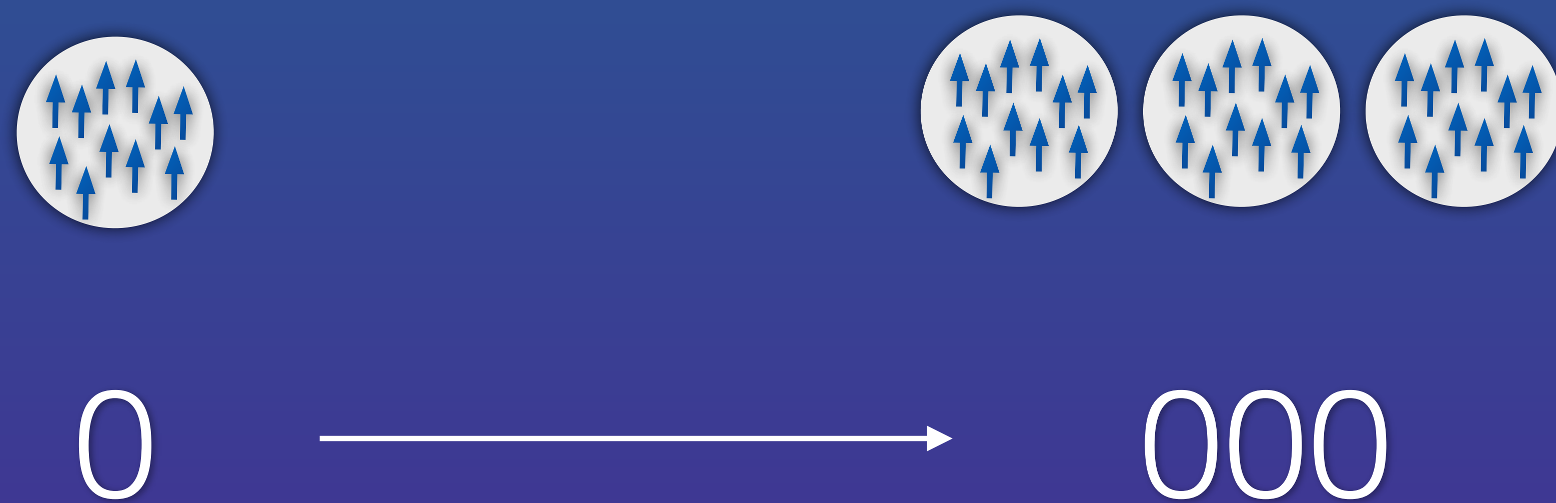
0



1



2- Bits can be cloned



3- Errors are discrete

0 ————————————> 1

1 ————————————> 0

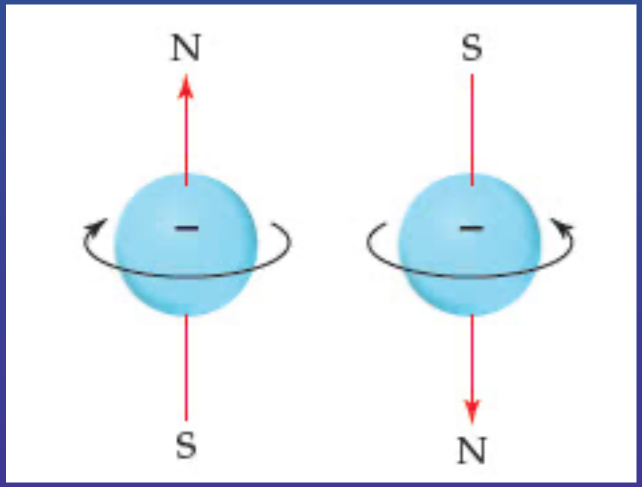
4- Bits can be observed

010 → 000

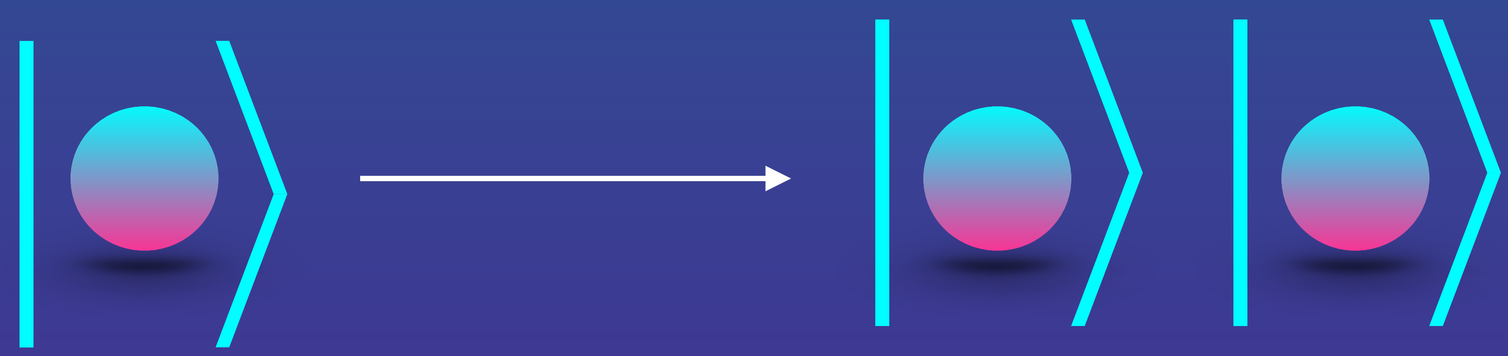
And corrected

Quantum bits have exactly the opposite properties

1-They are microscopic



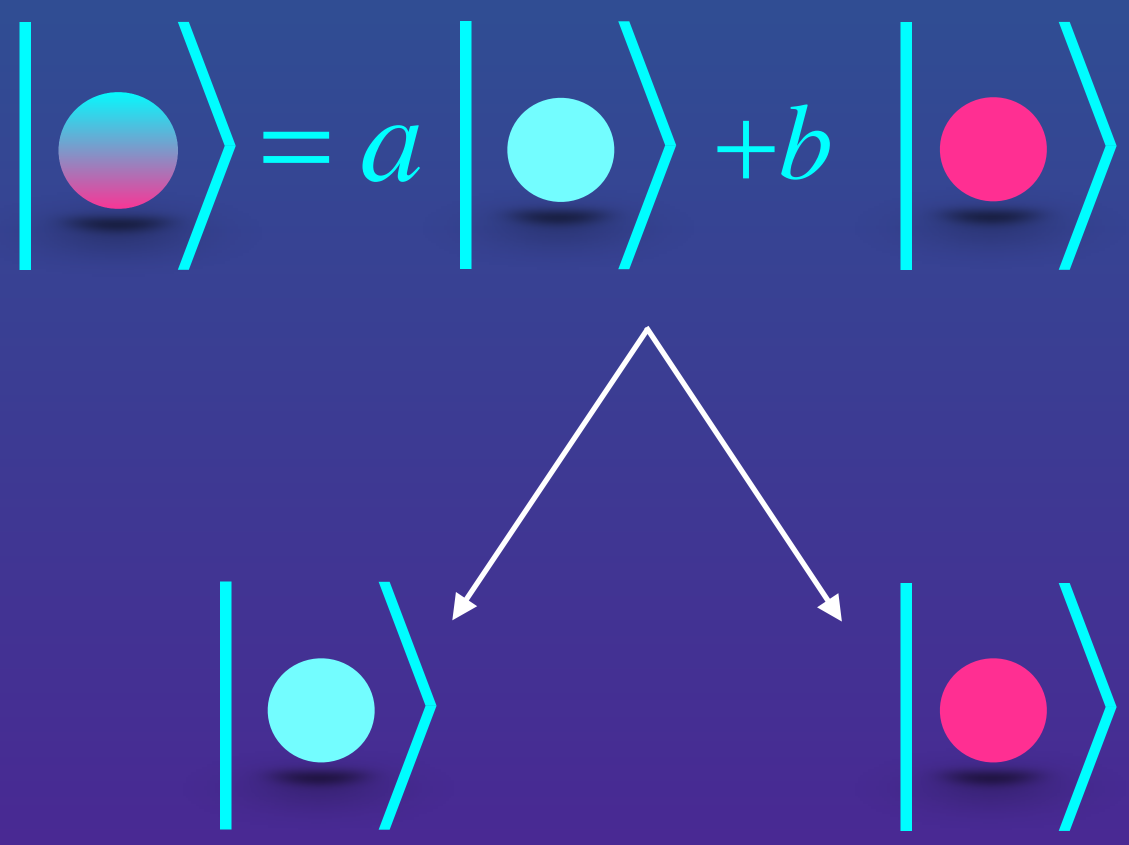
2-They cannot be cloned



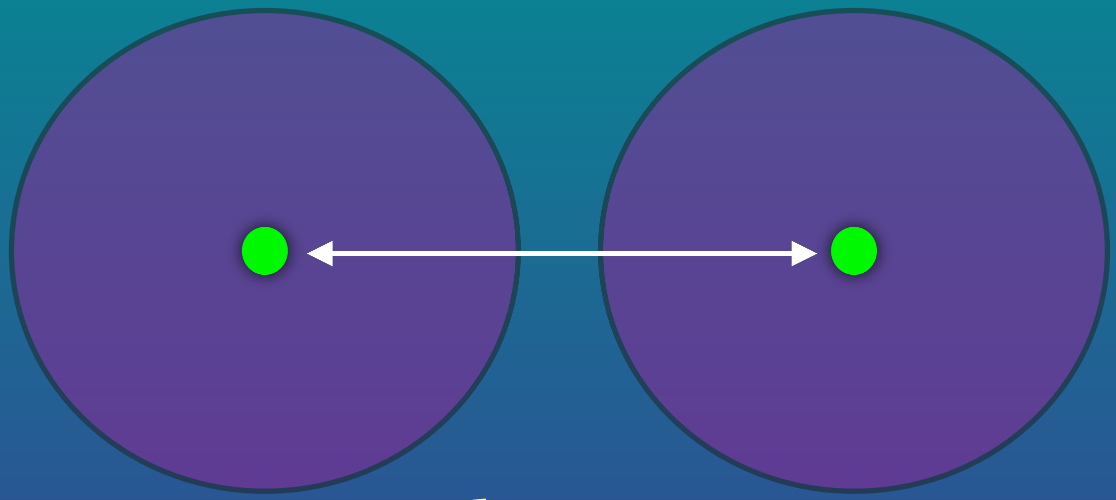
$$|\psi\rangle \otimes |0\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle$$

3-Quantum Errors are continuous

4-They cannot be observed



Classical Error Correction



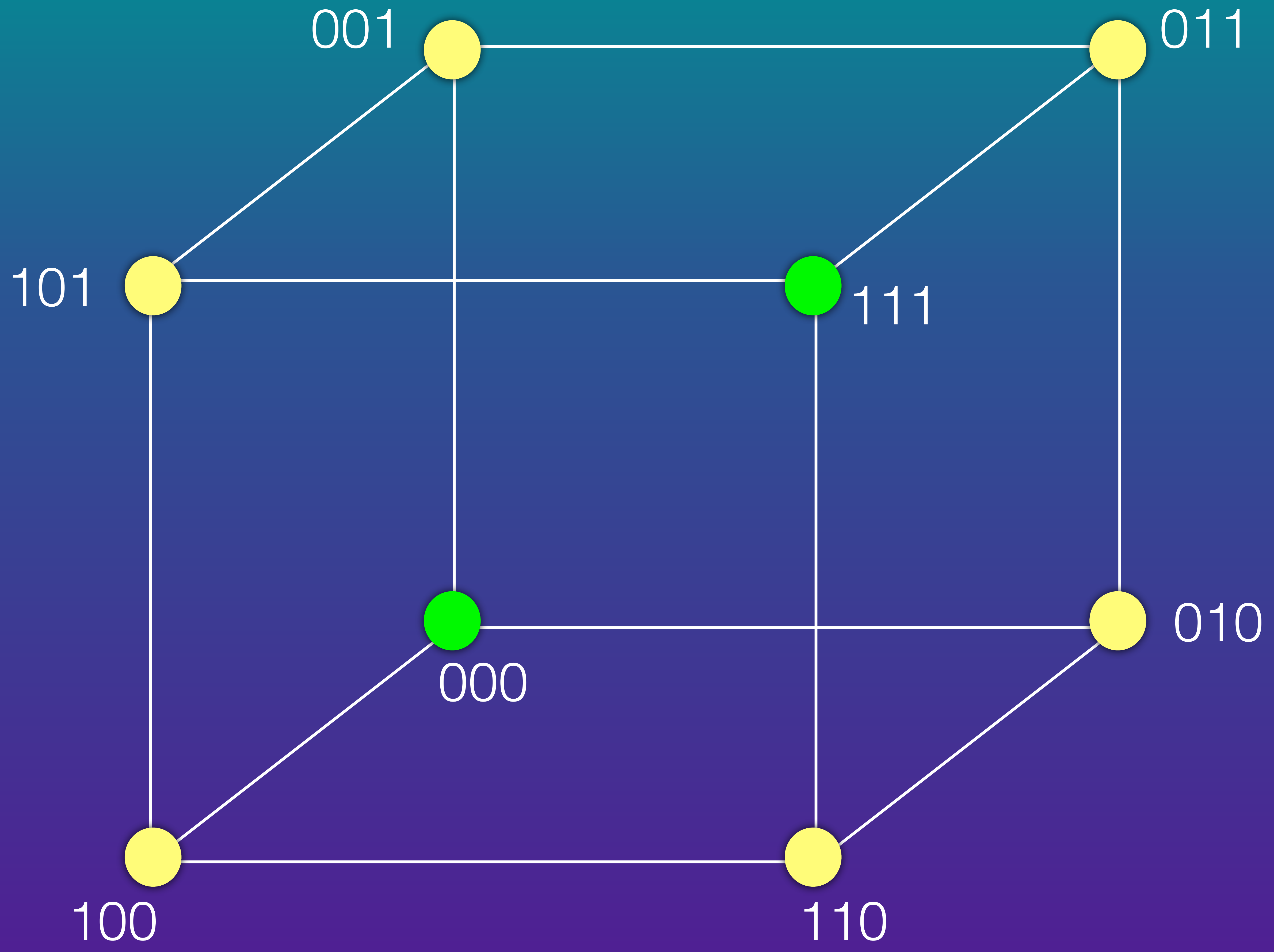
$d = 3$

$$0 \longrightarrow 000$$

$$p \longrightarrow 3p^2(1-p) + p^3 \sim 3p^2$$

$$1 \longrightarrow 111$$

Probability of error for repetition code.


001
011
101
111
000
010
100
110

$$V_3 = \{000,\ 001,\ 010,\ 011,\ 100,\ 101,\ 110,\ 111\}$$

$$C = \{000,\ 111\}$$

So we select only two codewords
from the set of 8 possible codewords

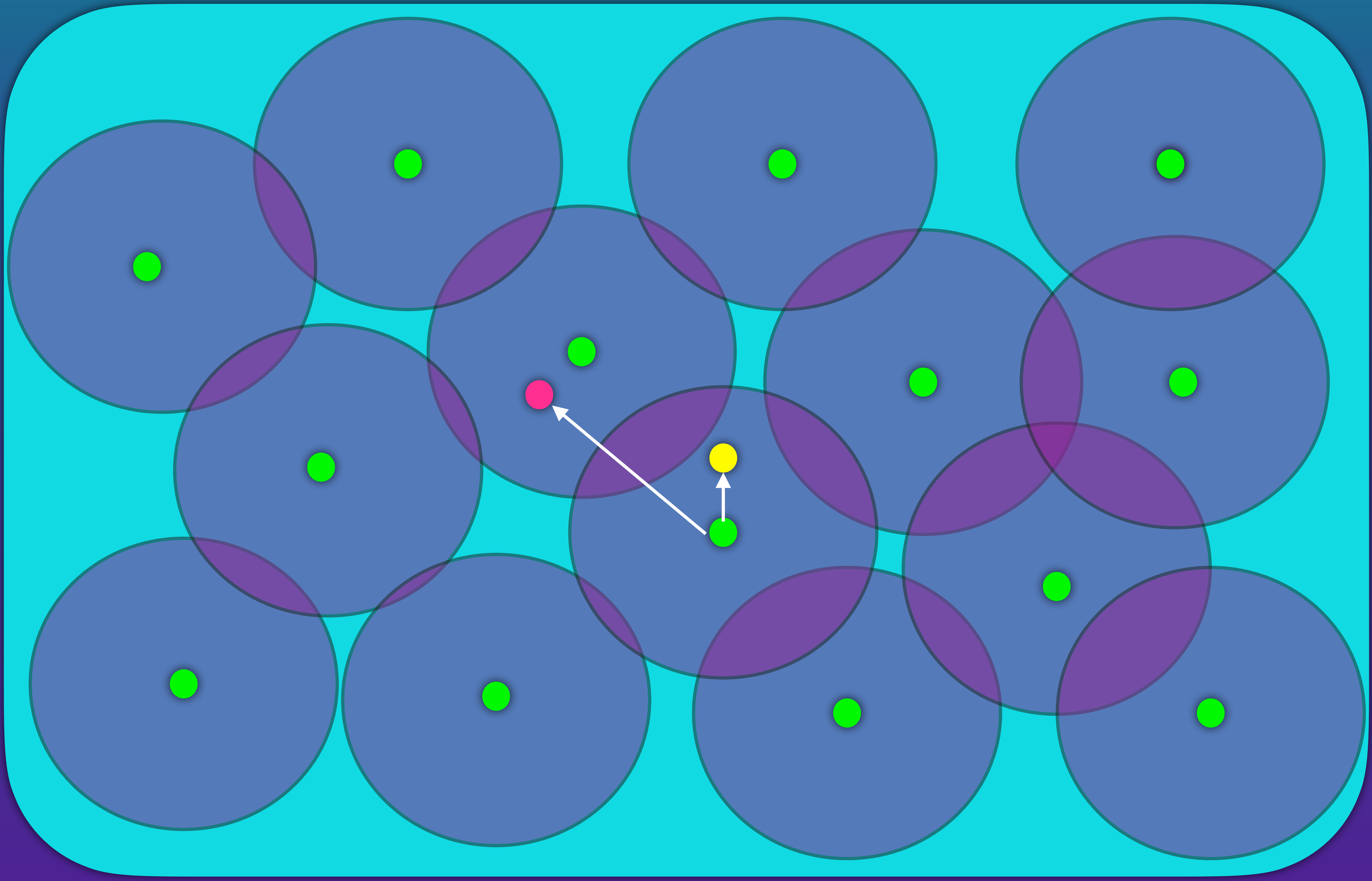
00	→	00000
01	→	10101
10	→	01010
11	→	11111

$$R = \frac{k}{n} = \frac{2}{5}$$

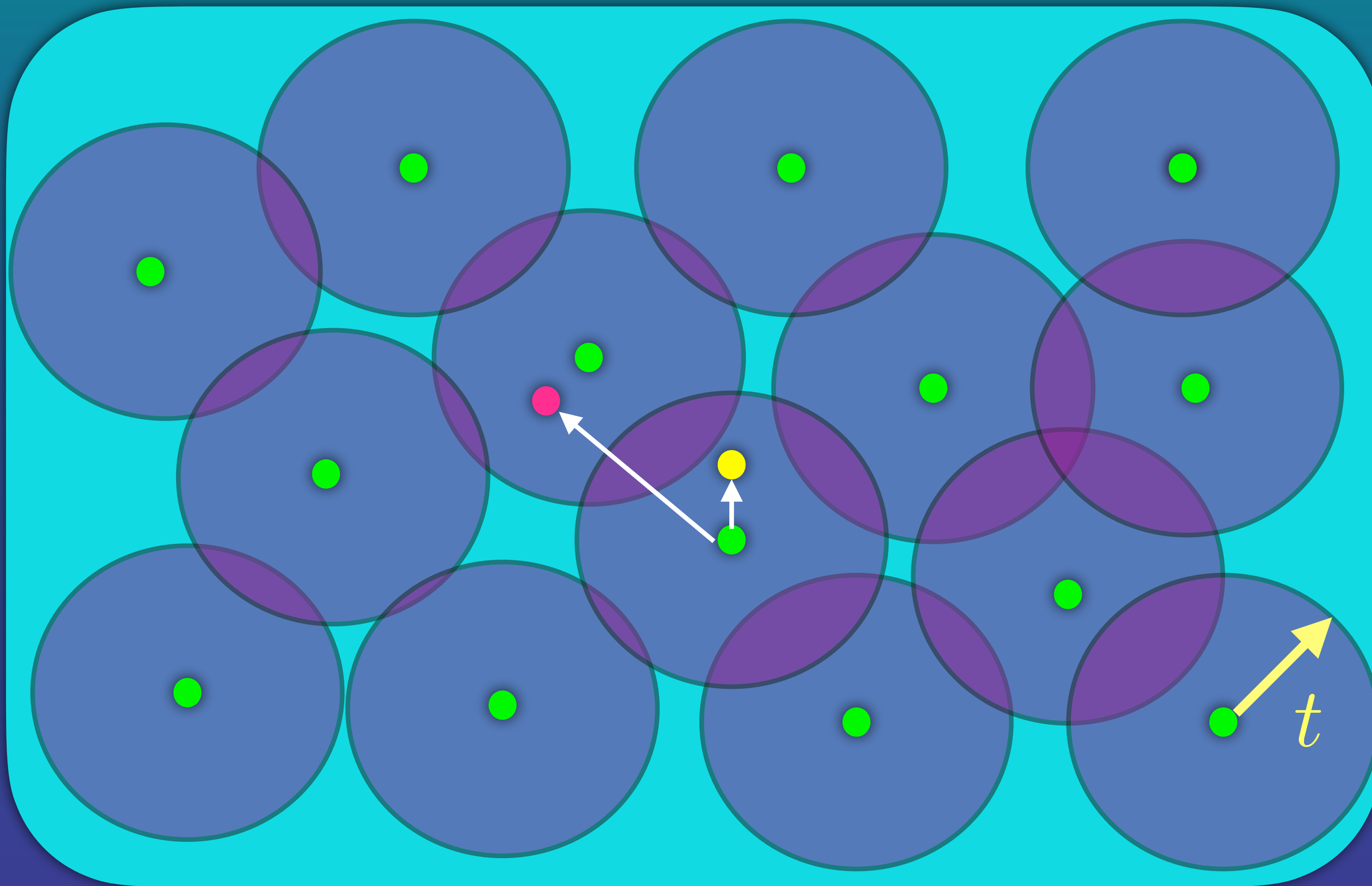
[n,k,d]=[5,2,2]

$$C = \{00000,\ 10101,\ 01010,\ 11111\}$$

Hamming Bound



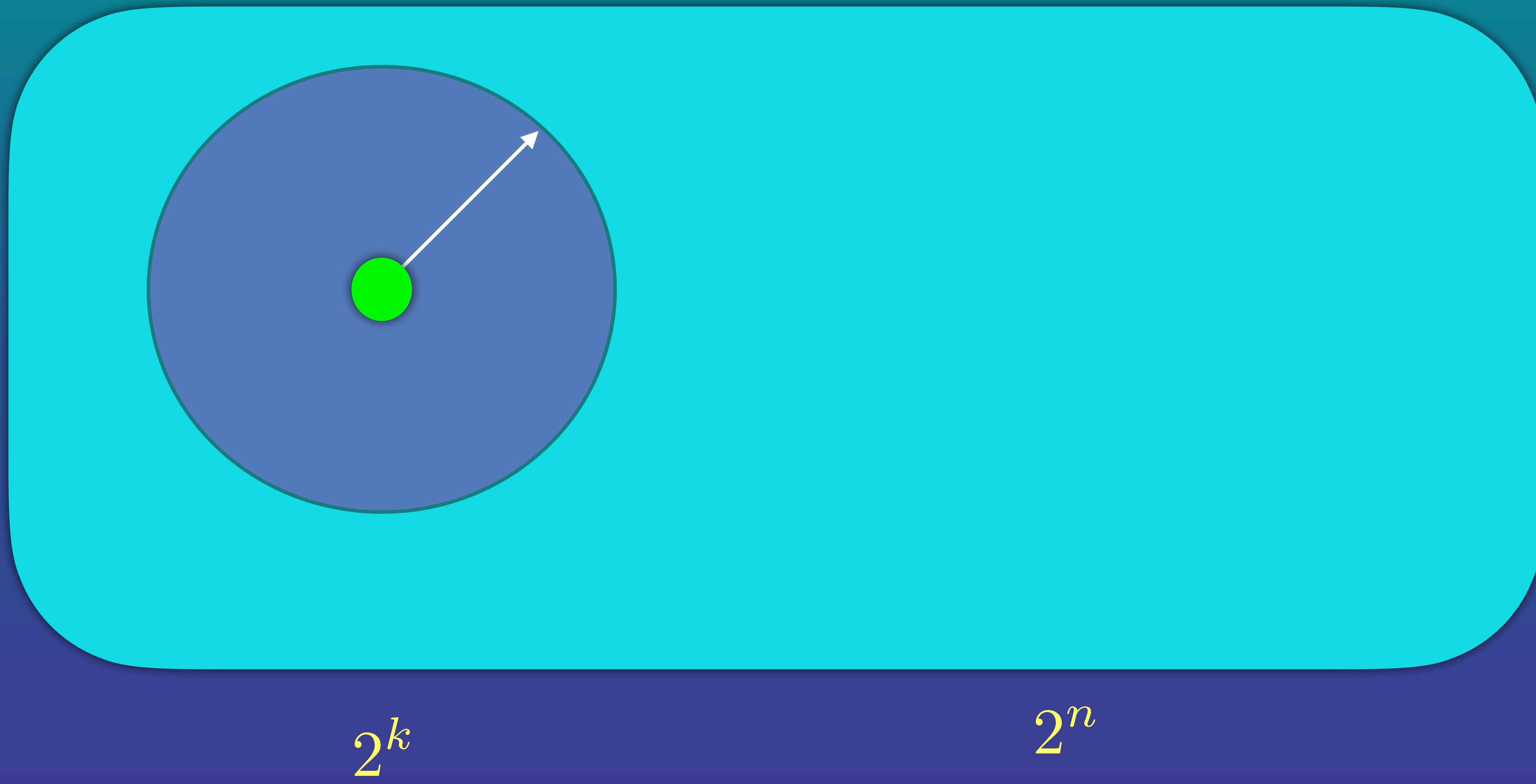
Hamming Bound



$$2^k \times V(n,t) < 2^n$$

The number of elements in each sphere.

$$V(n,t) = 1 + \binom{n}{1} + \binom{n}{2} + \cdots \binom{n}{t}$$

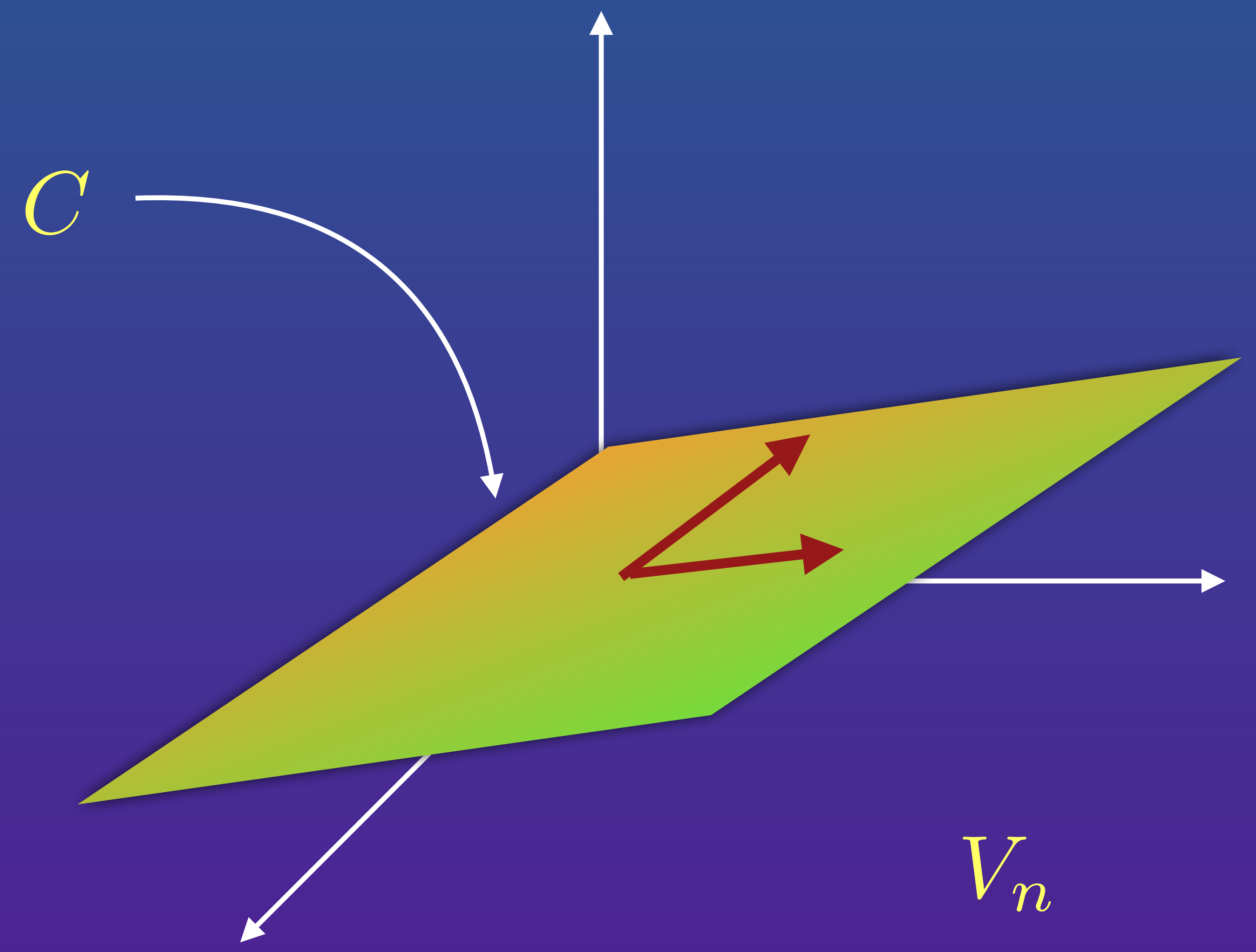


$$2^k \times V(n,t) < 2^n$$

$$V(n,t) = 1 + \binom{n}{1} + \binom{n}{2} + \cdots \binom{n}{t}$$

Linear Codes

The code space is chosen to be a subspace of the space of all codewords.



Linear Codes

00 → 00000			00 → 00000	
01 → 10101			01 → 10101	
10 → 01010			10 → 01010	
11 → 11111			11 → 11110	

A linear code

A non-linear code

Linear Codes

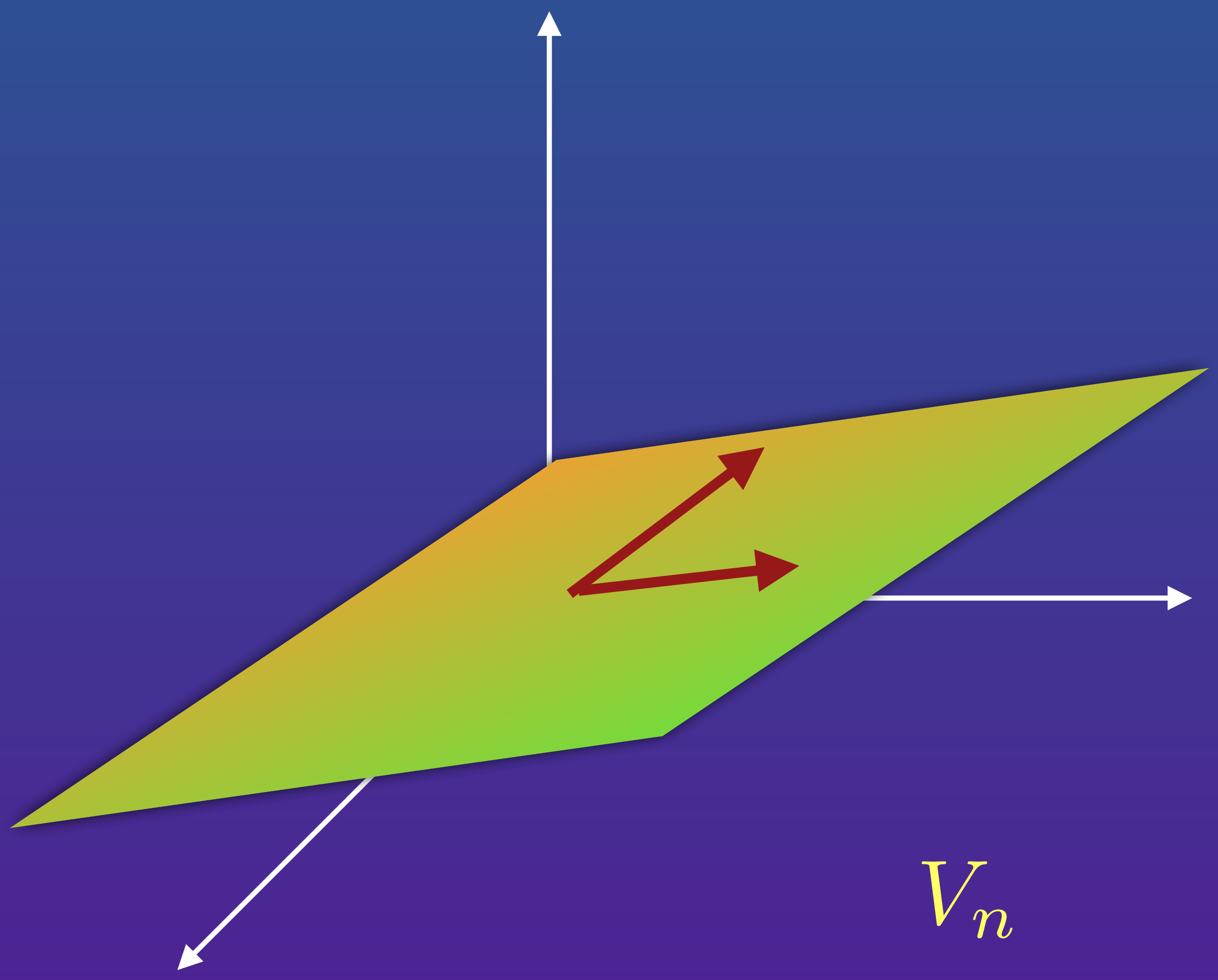
The basis of the total space

$$e_1 = (1, 0, 0, \cdots 0)$$

$$e_2 = (0, 1, 0, \cdots 0)$$

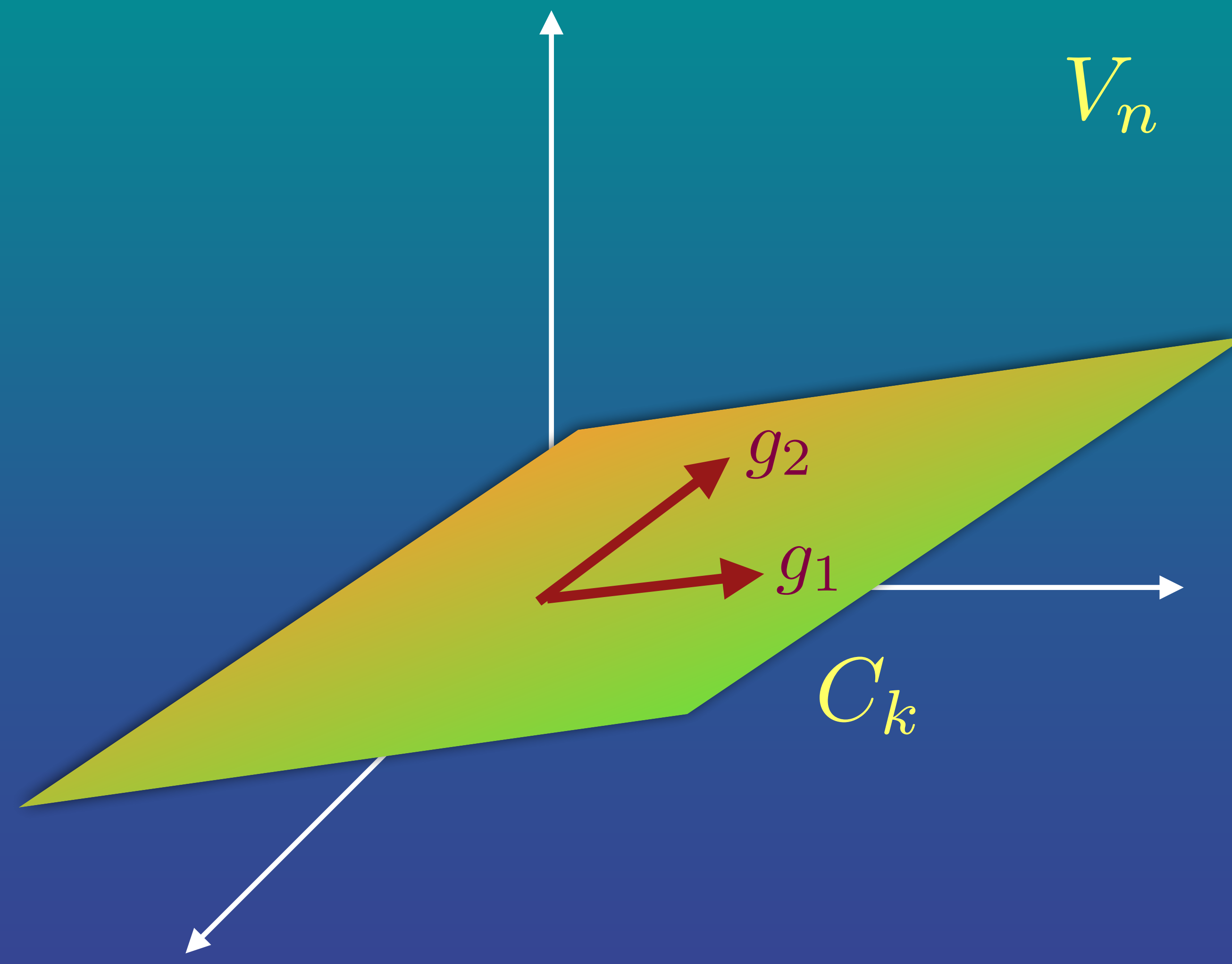
....

$$e_n = (0, 0, 0, \cdots 1)$$



The basis of code space

$$\begin{pmatrix} g_1 \\ g_2 \\ \cdot \\ g_k \end{pmatrix}$$



$$w = \alpha_1 g_1 + \alpha_2 g_2 + \cdots \alpha_k g_k$$

$$(\alpha_1,\ \alpha_2, \cdots,\ \alpha_k) \longrightarrow (w_1,\ w_2, \cdots,\ w_n)$$

$$w = \alpha_1 g_1 + \alpha_2 g_2 + \cdots \alpha_k g_k$$

$$(\alpha_1,\ \alpha_2, \cdots,\ \alpha_k) \longrightarrow (w_1,\ w_2, \cdots,\ w_n)$$

K bits are encoded into n bits.

Or in compact notation

$$\alpha \longrightarrow w = \alpha G$$

$$00 \longrightarrow 00 \cdots 0$$

$$10 \longrightarrow g_1$$

$$01 \longrightarrow g_2$$

$$11 \longrightarrow g_1 + g_2$$

$$w = \alpha_1 g_1 + \alpha_2 g_2 + \cdots \alpha_k g_k$$

$$\alpha \longrightarrow w = \alpha G$$

$$G = \begin{pmatrix} g_1 \\ g_2 \\ \cdot \\ g_k \end{pmatrix}_{k \times n}$$

$G =$ Generator Matrix

H is made of basis of orthogonal space

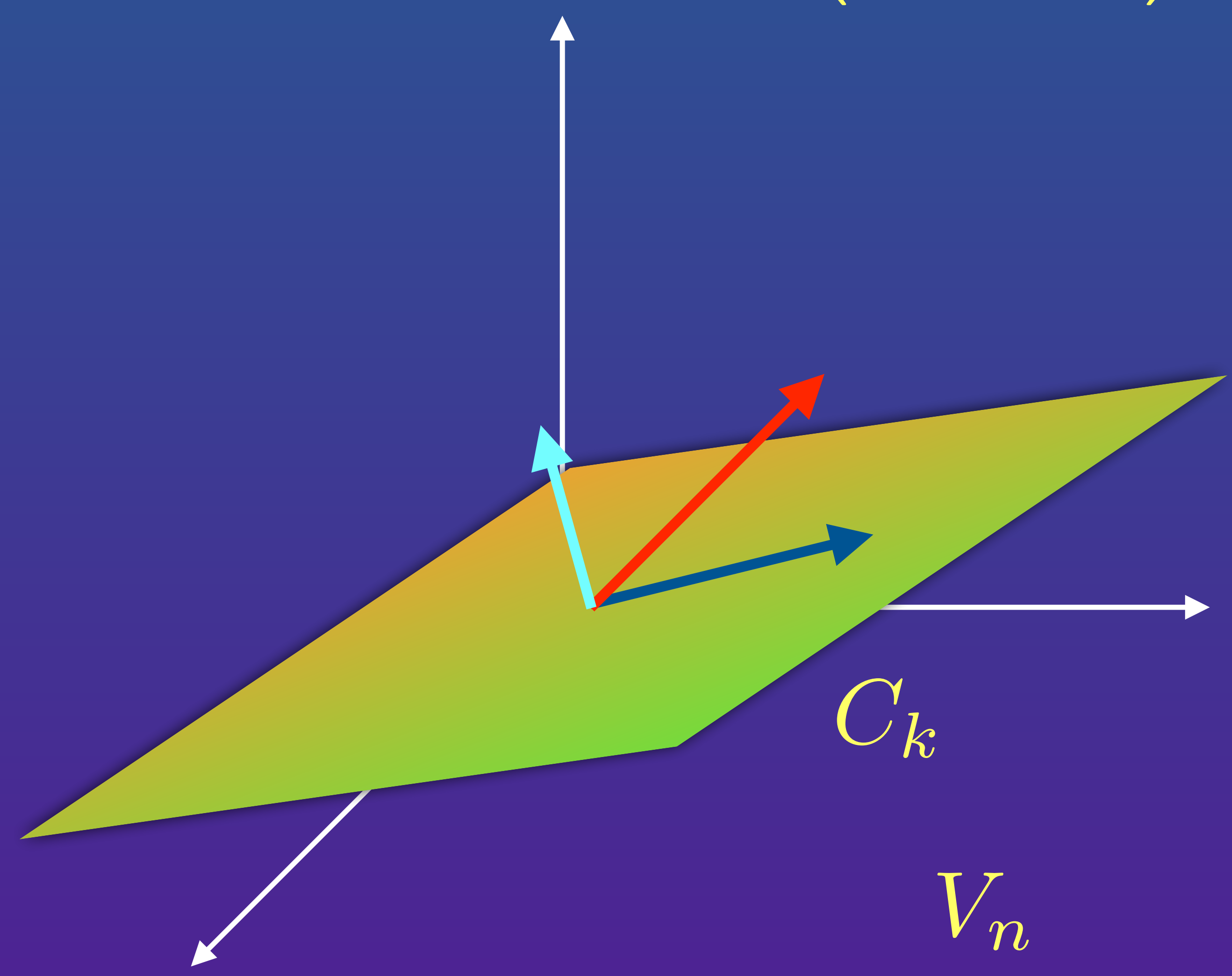
$$g_i \cdot h_j = 0$$

$$G = \begin{pmatrix} g_1 \\ g_2 \\ \cdot \\ g_k \end{pmatrix} \qquad H = \begin{pmatrix} h_1 \\ h_2 \\ \cdots \\ \cdots \\ h_{n-k} \end{pmatrix}$$

$$GH^T = 0$$

$$\omega H^T = \alpha G H^T = 0$$

$$wH^T = 0$$

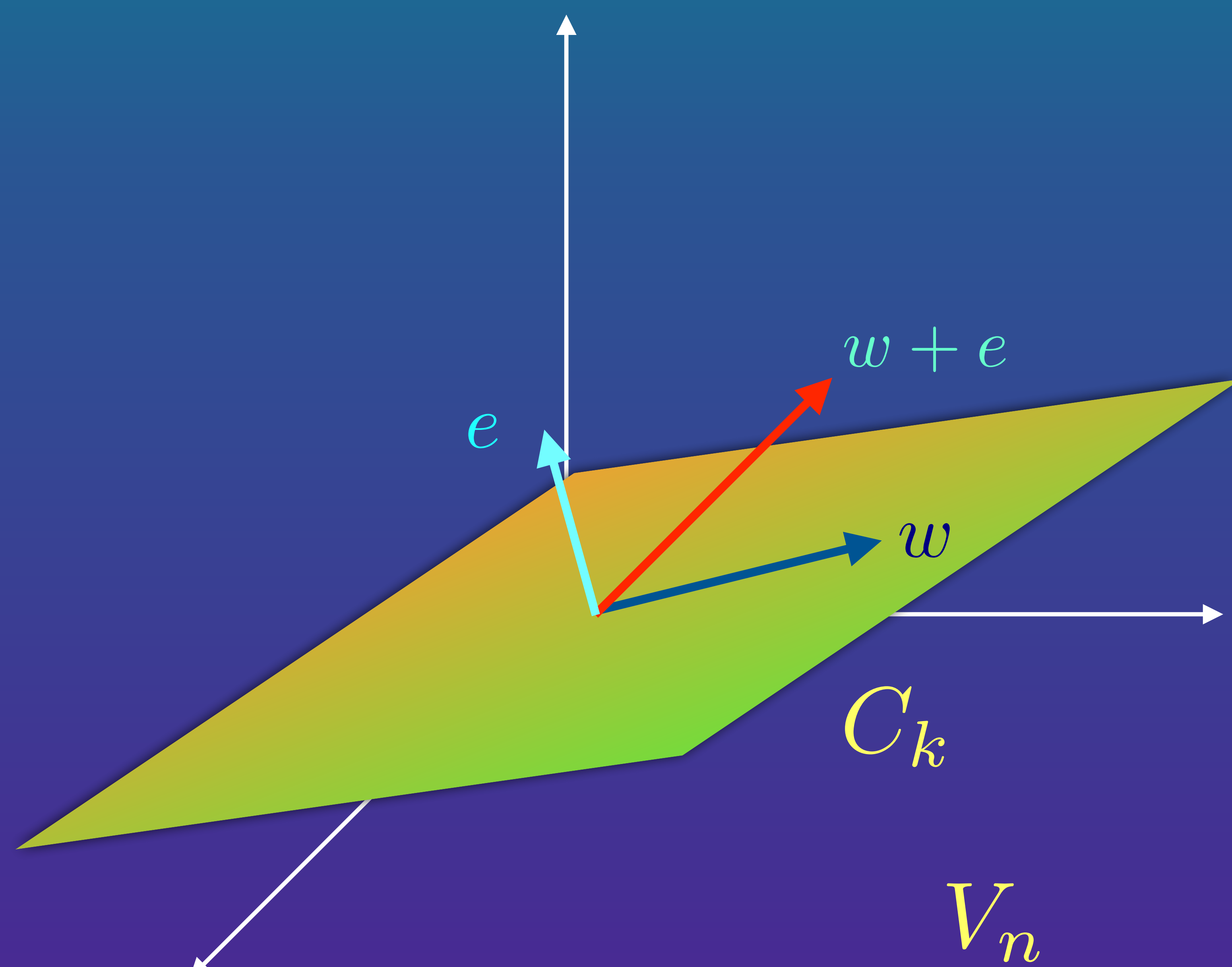


This is the syndrome of the error

$$wH^T = 0$$

No error

$$(w+e)H^T = eH^T$$

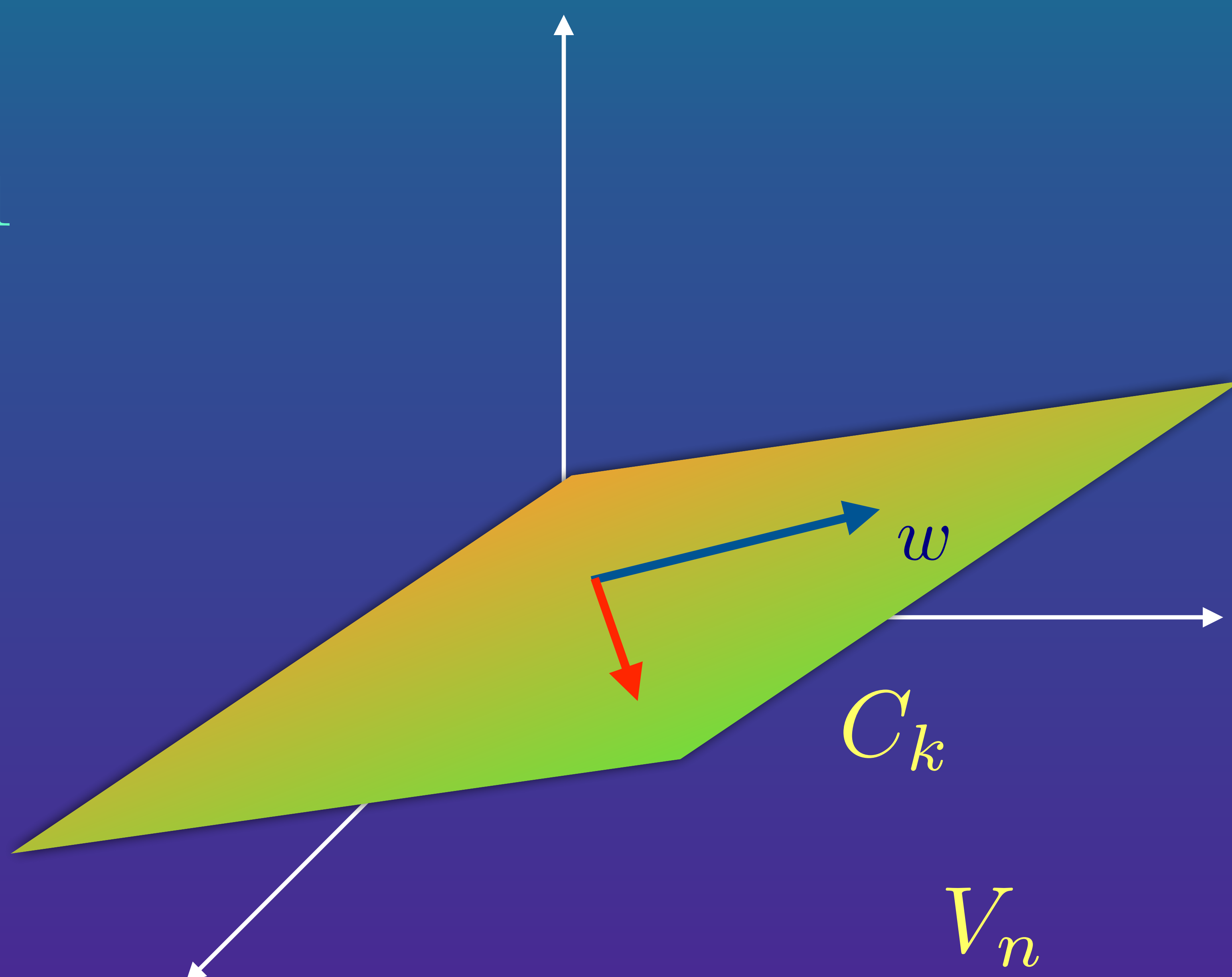


Un-detectable error

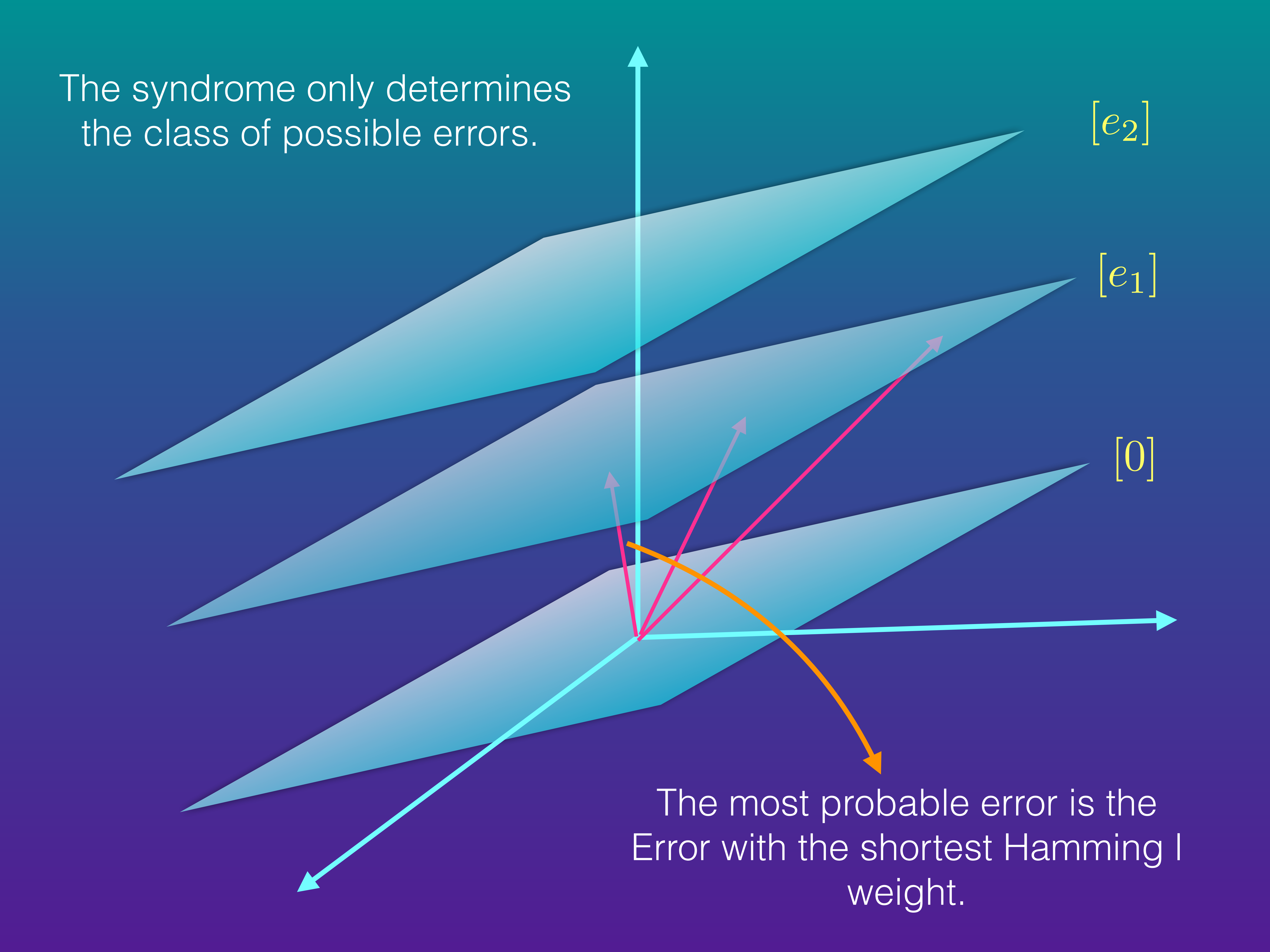
Logical Gate

$$000 \longrightarrow 111$$

$$\bar{0} \longrightarrow \bar{1}$$



If an error moves the state within the code space, it cannot be detected. It acts like a logical gate.


The syndrome only determines the class of possible errors.
$[e_2]$
$[e_1]$
$[0]$
The most probable error is the Error with the shortest Hamming l weight.

Quantum Error Correction

Notations

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

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

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

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

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

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

$$X|+\rangle = |+\rangle$$

$$X|-\rangle = -|-\rangle$$

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

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

$$Z|0\rangle = |0\rangle \qquad Z|1\rangle = -|1\rangle \qquad Z^t|s\rangle = (-1)^{ts}|s\rangle$$

$$X|0\rangle = |1\rangle \qquad X|1\rangle = |0\rangle \qquad X^t|s\rangle = |s+t\rangle$$

The first insight

Quantum errors are NOT continuous, they are discrete

$$\Omega = I \otimes U_0 + X \otimes U_1 + Y \otimes U_2 + Z \otimes U_3$$

$$\Omega(|\psi\rangle \otimes |e\rangle) = |\psi\rangle \otimes U_0|e_0\rangle + X|\psi\rangle \otimes |e_1\rangle + Y|\psi\rangle \otimes |e_2\rangle + Z|\psi\rangle \otimes |e_3\rangle$$

Ω

$$P(X) = \langle e_1|e_1\rangle$$

$$P(Y) = \langle e_2|e_2\rangle$$

$$P(Z) = \langle e_3|e_3\rangle$$

The simplest example of a quantum code

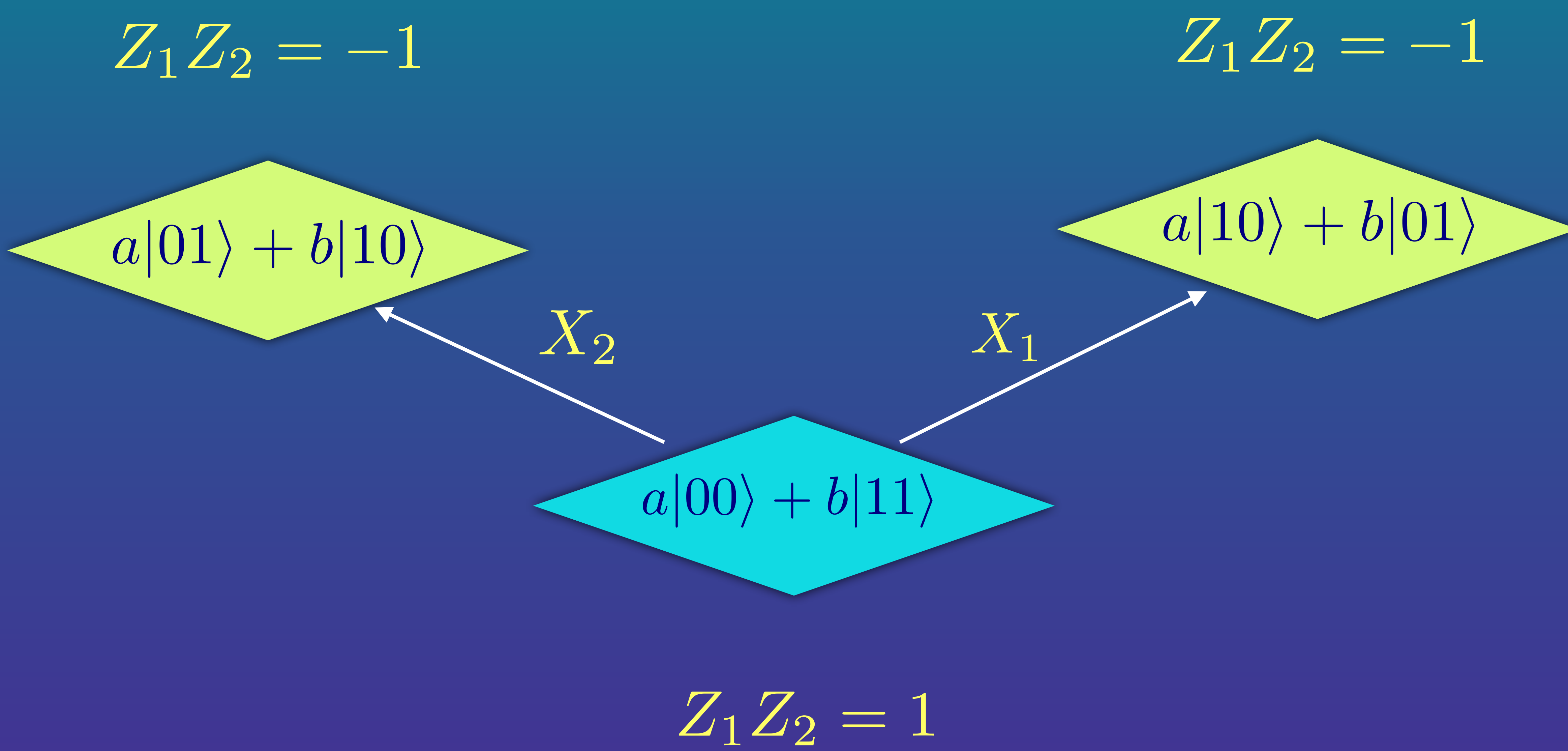
$$|0\rangle \longrightarrow |00\rangle$$

$$|1\rangle \longrightarrow |11\rangle$$

$$a|0\rangle + b|1\rangle \longrightarrow a|00\rangle + b|11\rangle$$

$$|\psi\rangle = \ a|0\rangle + b|1\rangle \longrightarrow a|00\rangle + b|11\rangle \ = |\overline{\psi}\rangle$$

$$Z_1 Z_2 |\overline{\psi}\rangle = |\overline{\psi}\rangle$$



This is an error-detecting code,
We do not know which error has occurred.

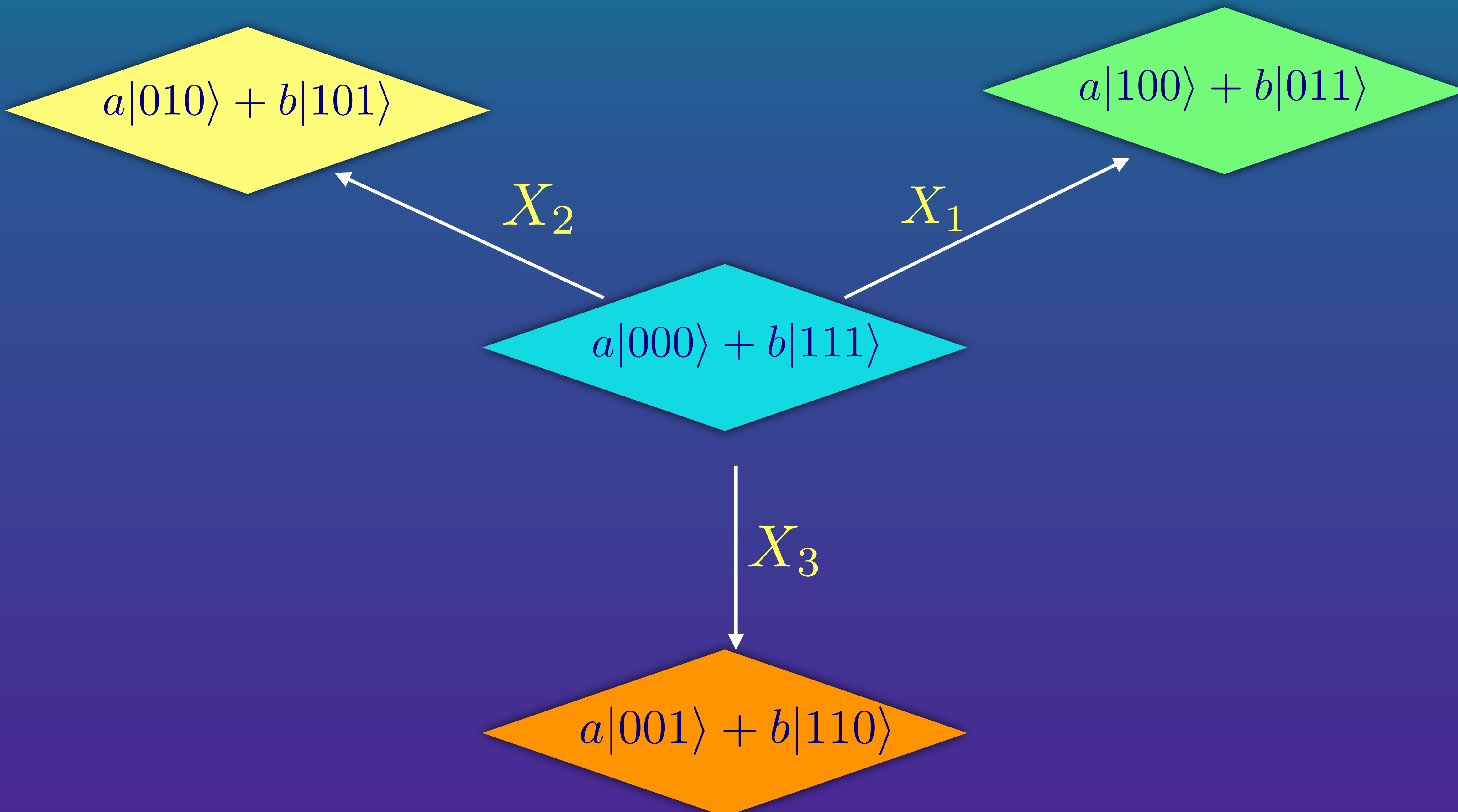
A better code

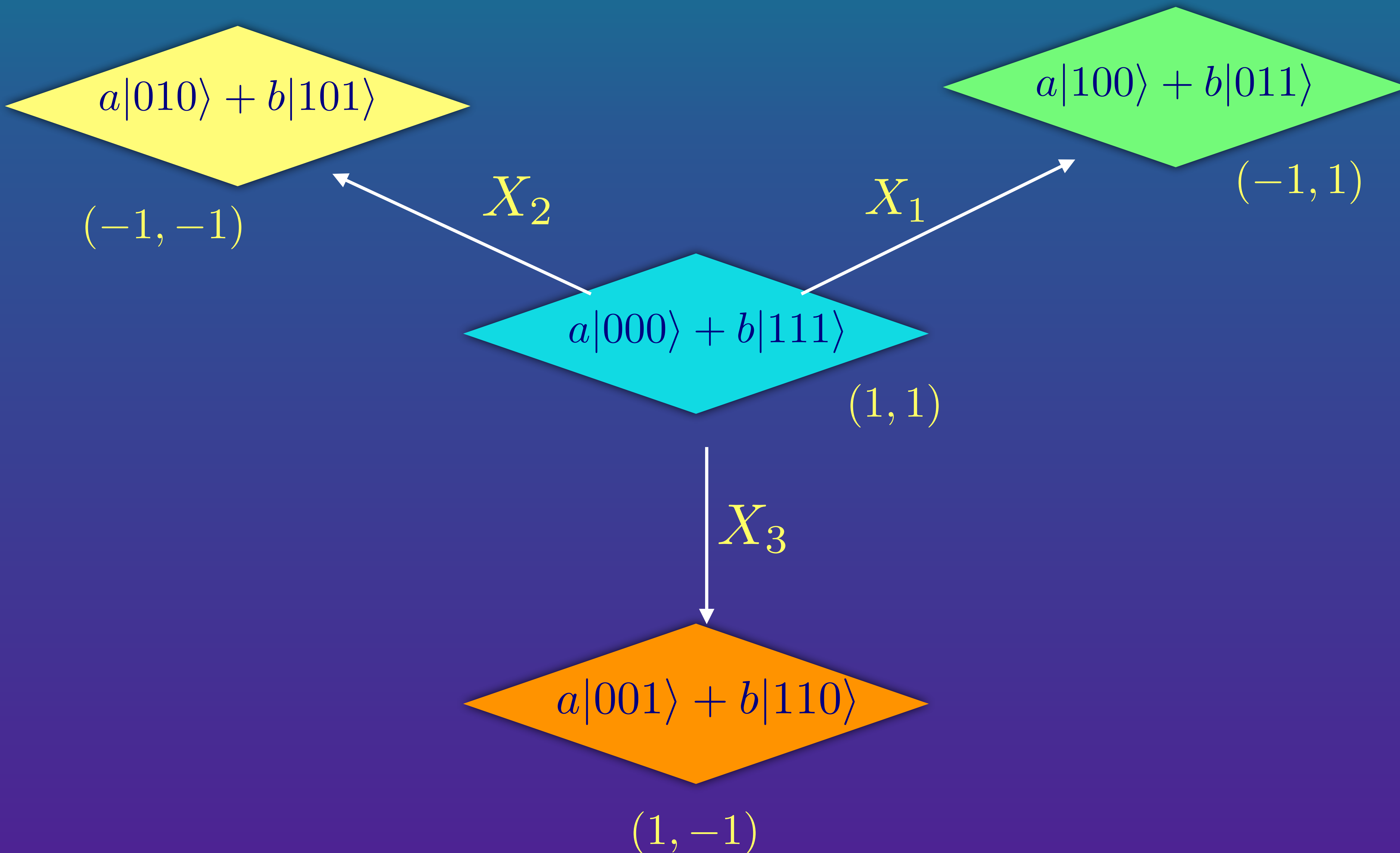
$$|0\rangle \longrightarrow |000\rangle$$

$$|1\rangle \longrightarrow |111\rangle$$

$$a|0\rangle + b|1\rangle \longrightarrow a|000\rangle + b|111\rangle$$

We determine only the error not the state itself.



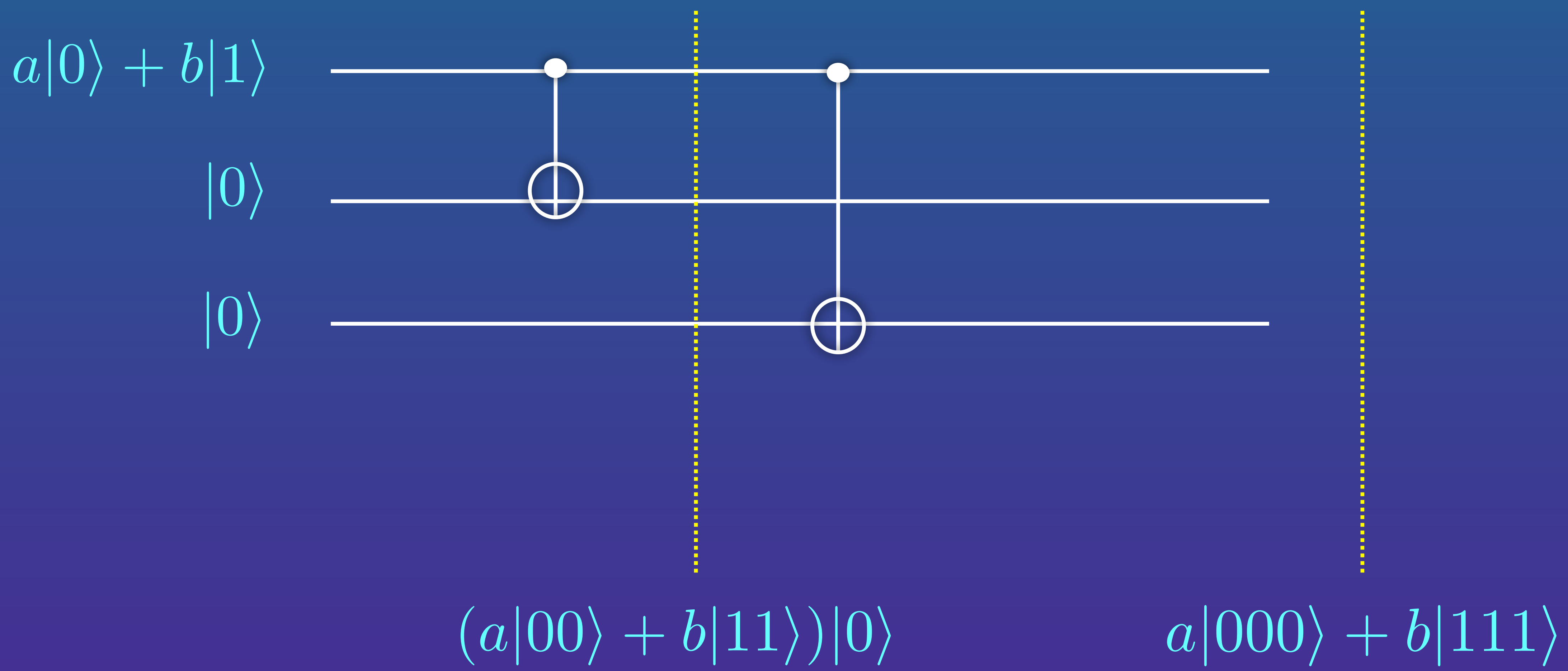

$a|010\rangle + b|101\rangle$
$(-1,-1)$
$a|100\rangle + b|011\rangle$
$(-1,1)$
X_2
X_1
$a|000\rangle + b|111\rangle$
$(1,1)$
X_3
$a|001\rangle + b|110\rangle$
$(1,-1)$

Syndromes.

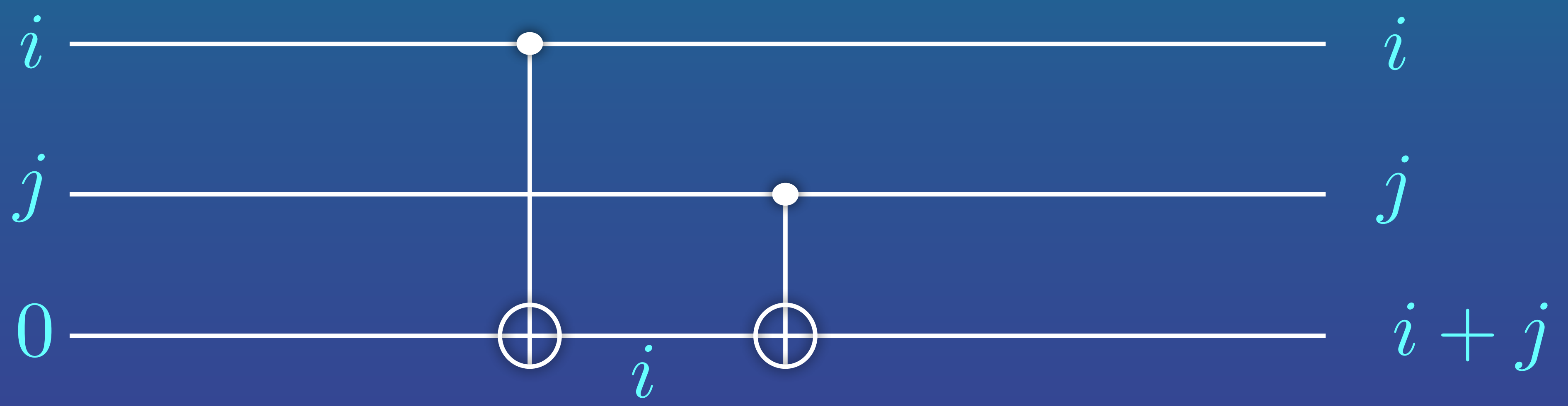
Bit flip errors

	$Z_1 Z_2$	$Z_2 Z_3$
I	+1	+1
X_1	-1	+1
X_2	-1	-1
X_3	+1	-1

Encoding Circuit



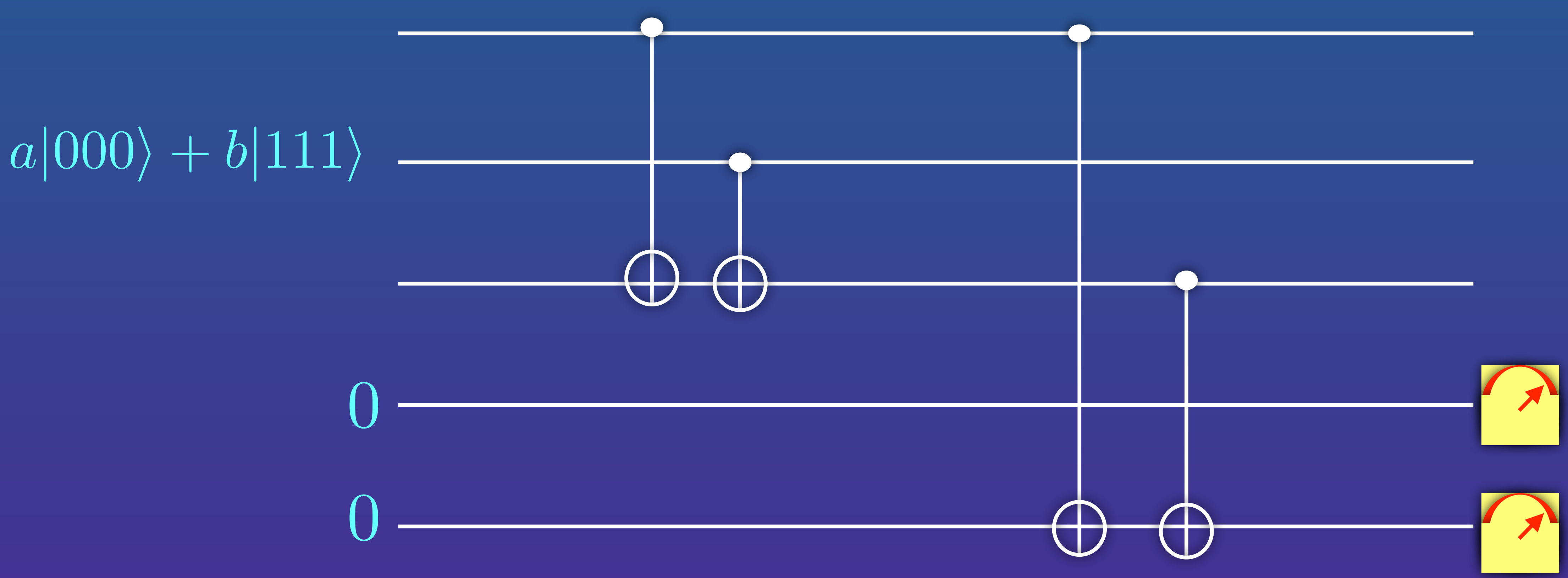
Measurement of $Z_1 Z_2$



$$CNOT|i, j\rangle = |i, i + j\rangle$$

If $i = j$ then $i + j$ = 0. So the last bit measures $Z_1 Z_2$.

Syndrome Measurement



A code for detecting phase errors

$$a|0\rangle + b|1\rangle \longrightarrow a|000\rangle + b|111\rangle$$

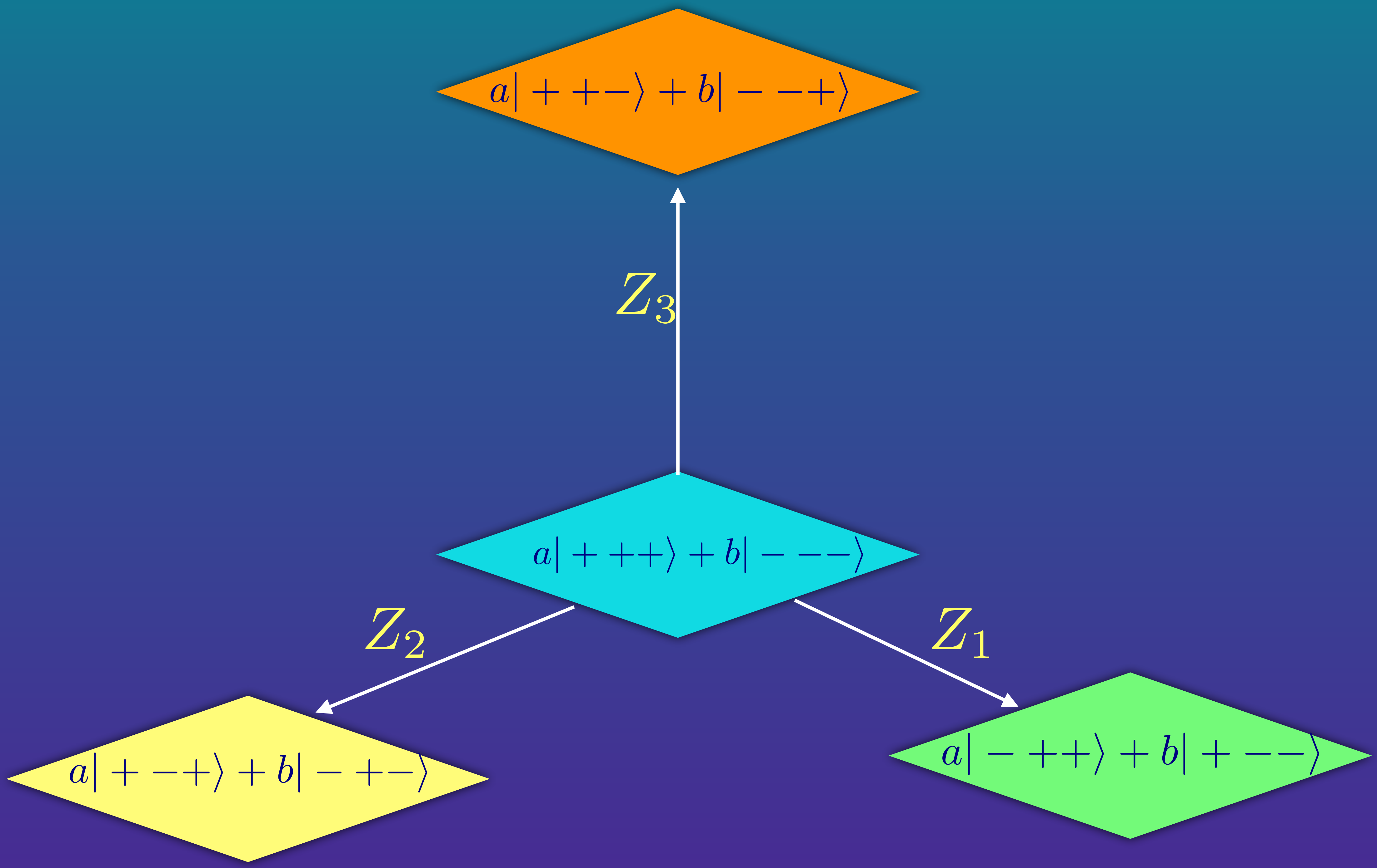
$$|\psi\rangle = a|000\rangle + b|111\rangle \xrightarrow{Z_1} a|000\rangle - b|111\rangle$$

The suitable code

$$|0\rangle \longrightarrow |+++\rangle$$

$$|1\rangle \longrightarrow |---\rangle$$

$$a|0\rangle + b|1\rangle \longrightarrow a|+++\rangle + b|---\rangle$$


$a|++-\rangle + b|--+\rangle$
Z_3
$a|+++\rangle + b|---\rangle$
Z_2
Z_1
$a|+-+\rangle + b|-+-\rangle$
$a|-++\rangle + b|+--\rangle$

	X_1X_2	X_1X_3
I	+1	+1
Z_1	-1	-1
Z_2	-1	+1
Z_3	+1	-1

The Shor Code

$$|0\rangle \longrightarrow (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$|1\rangle \longrightarrow (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle| - 111\rangle)$$

We can detect bit flip errors
in each Bloch in the same way as before.

$$|0\rangle \longrightarrow (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$|1\rangle \longrightarrow (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle| - 111\rangle)$$

$$(|100\rangle + |011\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + ||111\rangle)$$

$$(|100\rangle - |011\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle| - |111\rangle)$$

$$Z_1 \quad \text{or} \quad Z_2 \quad \text{or} \quad Z_3$$

Have the same effect on each Bloch.

$$|0\rangle \longrightarrow (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$(|000\rangle - |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + ||111\rangle)$$

$$X_I = X_1X_2X_3$$

$$X_{II} = X_4X_5X_6$$

$$X_{III} = X_7X_8X_9$$

These two syndromes determine in which block a phase error has occurred.

$$X_IX_{II} \qquad X_{II}X_{III}$$

Why do we care only about X and Z errors

and not Y errors?

$$\langle\psi|Z|\psi\rangle = 0$$

Diff. a Z error from no error

$$\langle\psi|X|\psi\rangle = 0$$

Diff. an X error from no error

$$\langle\psi|XZ|\psi\rangle = 0$$

Diff. an X error from a Z error

$$\langle\psi|Y|\psi\rangle = 0$$

$$\langle\psi|YZ|\psi\rangle = 0$$

Due to the properties of Pauli operators:

$$\langle\psi|YX|\psi\rangle = 0$$

The 5 Qubit Code

Now all the syndromes are different

$$s_1 = Z\ I\ Z\ X\ X$$

$$s_2 = I\ Z\ X\ X\ Z$$

$$s_3 = Z\ X\ X\ Z\ I$$

$$s_4 = X\ X\ Z\ I\ Z$$

CSS Codes

Why we don’t use the ideas of classical linear codes

to invent quantum codes?

How?

How?

$$w = \sum_i \alpha_i g_i$$

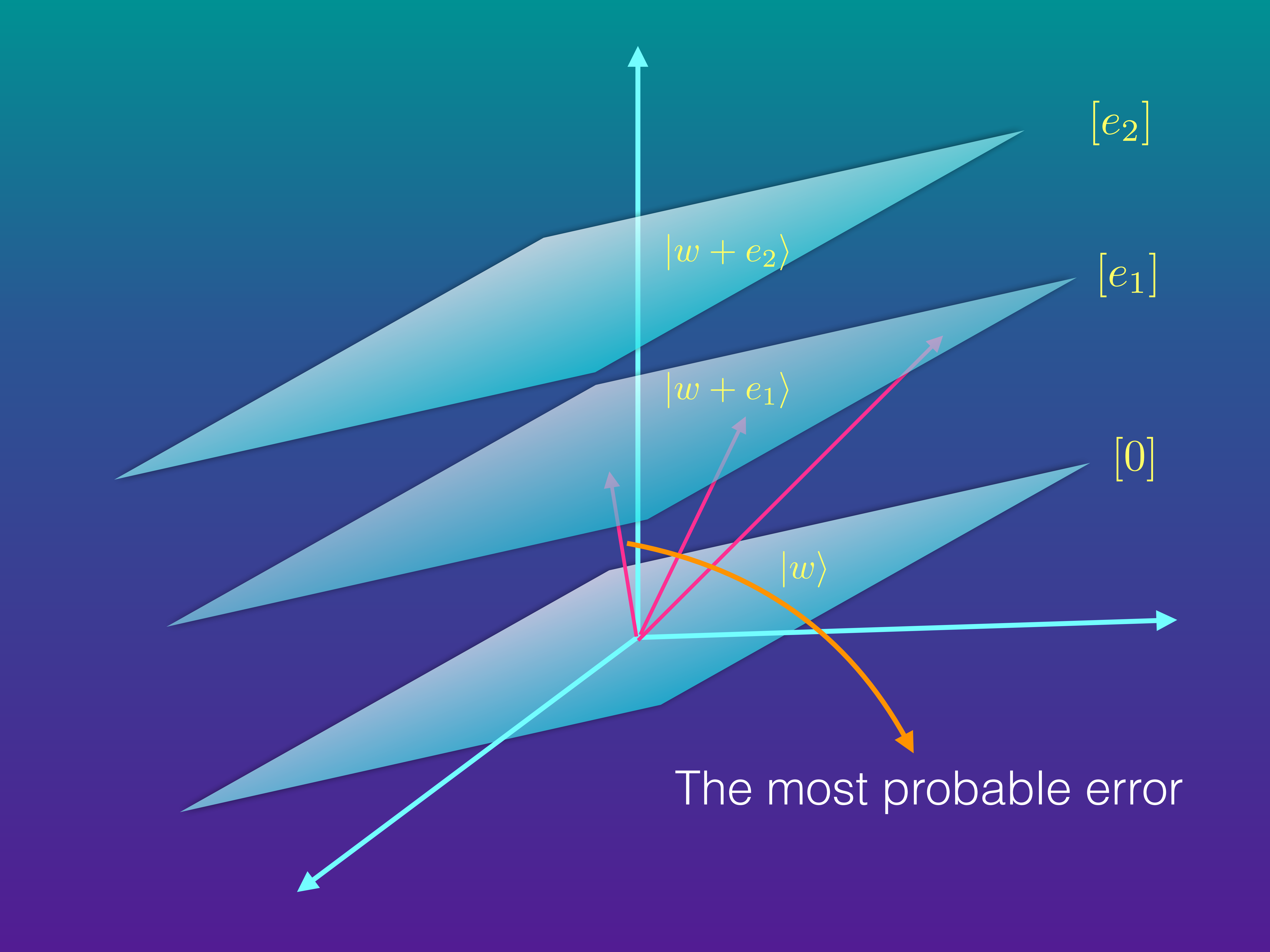
$$\alpha_i = 0\ ,\ 1$$

$$g_i = (0\ 1\ 0\ 1\ 1\ 0\ 1)$$

$$|w\rangle = \sum_i \alpha_i |g_i\rangle$$

$$\alpha_i \in \text{Complex numbers}$$

$$|g_i\rangle = |0\ 1\ 0\ 1\ 1\ 0\ 1\rangle$$



$[e_2]$
$|w + e_2\rangle$
$[e_1]$
$|w + e_1\rangle$
$[0]$
$|w\rangle$
The most probable error

$$\text{Classical Error}: \; w \longrightarrow w + e$$

$$e = (1\ 1\ 0\ 0\ 0)$$

$$\text{Quantum (bit Flip) error}: \; |w\rangle \longrightarrow |w + e\rangle$$

$$X^e = X\ X\ I\ I\ I$$

We can use this technique for bit flip errors.

But how should we combat phase flip errors?

We will show this in the second part.

Thank you for your attention