INTRODUCCIÓN A LOS CÓDIGOS CORRECTORES DE ERRORES CUÁNTICOS

DIEGO RUANO

SEMINARIO DE ÁLGEBRA, GEOMETRÍA ALGEBRAICA Y SINGULARIDADES

UNIVERSIDAD DE LA LAGUNA, 22/3 2022

imUVa Mathematics Research Institute

Universidad de Valladolid

OUTLINE OF THE TALK

- CLASSICAL ERROR CORRECTING CODES
- QUANTUM INFORMATION PROCCESSING
- QUANTUM ERROR CORRECTION
  - SHOR CODE
  - CSS CONSTRUCTION

CLASSICAL COMMUNICATION CHANNEL

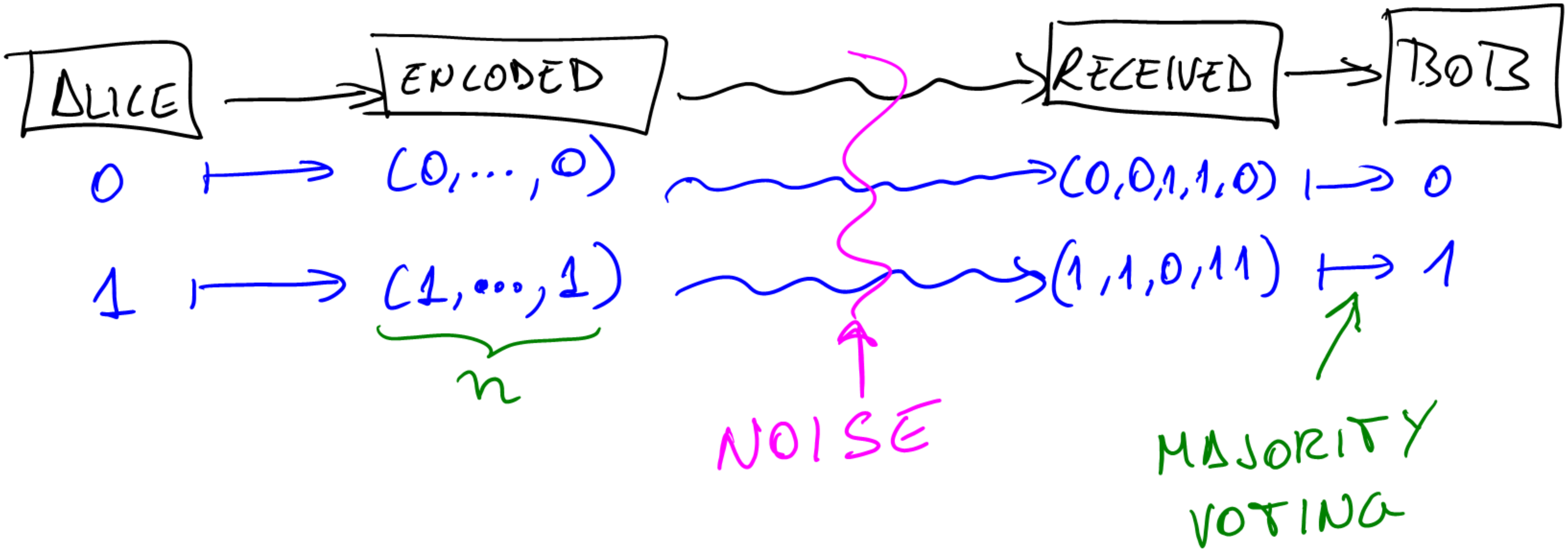
BITS 0, 1 — BINARY SYMMETRIC CHANNEL

ALICE	→	BOB	WITH PROBABILITY
0	→	0	$(1-P)$
0	→	1	P
1	→	0	P
1	→	1	$(1-P)$

ERROR WITH PROBABILITY $P < \frac{1}{2}$

ERRORS IN DIFFERENT BITS ARE STATISTICALLY INDEPENDENT

REPETITION CODE



Ex: $n=5$ WE CAN CORRECT UP TO 2 ERRORS

(IN GENERAL $\left\lfloor \frac{n-1}{2} \right\rfloor$)

LINEAR BLOCK CODES

$$
\begin{array}{ccccccccc}
\mathbb{F}_q^k & \xrightarrow[\text{ENCODING}]{G} & \mathbb{F}_q^n & \xrightarrow{\text{NOISE}} & \mathbb{F}_q^n & \xrightarrow{\text{DECODING}} & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^k \\
\vec{x} & \longmapsto & \vec{c} & \longmapsto & \vec{r} & \longmapsto & \vec{c} & \longmapsto & \vec{x} \\
\text{MESSAGE} & & \text{ENCODED} & & \parallel & & & & \\
 & & & & \vec{c}+\vec{e} & & & &
\end{array}
$$

$\vec{c} = G\vec{x}$

G $k \times n$ GENERATOR MATRIX

WE MAY THINK IN $G = (\mathrm{Id} \mid A)$

$$\vec{c} = \underbrace{(\underbrace{\vec{x}}_{k}, \underbrace{****}_{n-k})}_{n}$$

$\mathcal{C} = \mathbb{F}_q^k \cdot G$ LINEAR CODE

IF THERE ARE NOT TOO MANY ERRORS

↳ WE CAN RECOVER $\vec{c}$

MINIMUM DISTANCE

- HAMMING WEIGHT $\quad w_H(\vec{x}) = \#\{i \mid x_i \neq 0\}$

- # ERRORS $= w_H(\vec{e})$

$$d_H(\vec{x},\vec{y}) = \#\{i \mid x_i \neq y_i\}$$

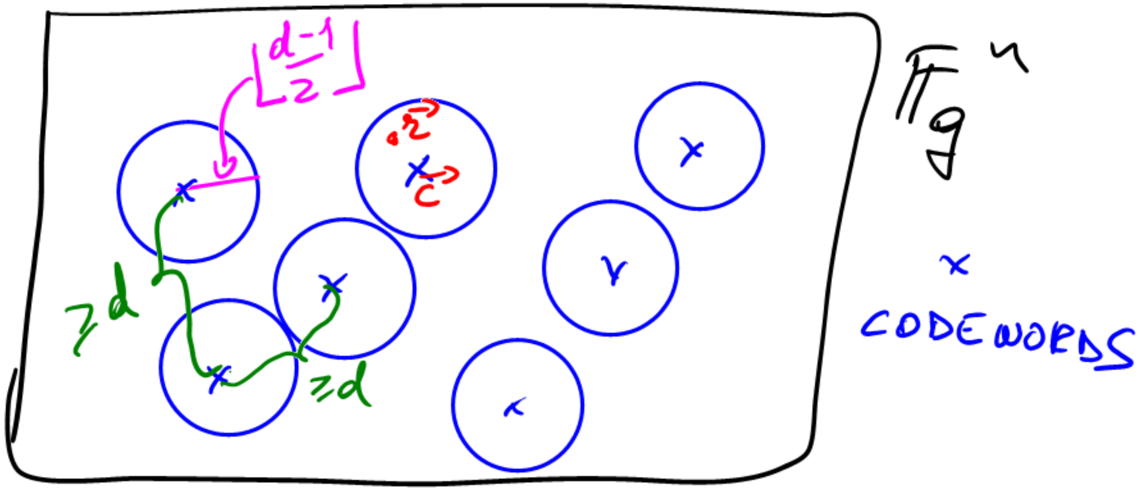
$$\underline{d(\mathcal{C})} = \min\{d_H(\vec{x},\vec{y}) \mid \vec{x},\vec{y} \in \mathcal{C}\}$$

$$= \min\{w_H(\vec{x}) \mid \vec{x} \in \mathcal{C} \setminus \{0\}\}$$

MINIMUN DISTANCE

WE CAN CORRECT UP TO

$$\left\lfloor \frac{d-1}{2} \right\rfloor \text{ ERRORS}$$



CODE'S PARAMETERS

$$[n, k, d]_q$$

LENGTH CODEWORDS

OF INFORMATION BITS

MINIMUM DISTANCE

FIXED n: $k \uparrow$ $d \uparrow$

$n-k$ REDUNDANT BITS

WE CAN CORRECT UP TO $\left\lfloor \frac{d-1}{2} \right\rfloor$ ERRORS

DUAL CODE (ORTHOGONAL)

$$\mathcal{C}^{\perp} = \{ \vec{x} \in \mathbb{F}_q^n \mid \vec{x} \cdot \vec{c} = \vec{0} \ \forall \vec{c} \in \mathcal{C} \}, \ \dim \mathcal{C}^{\perp} = n-k$$

H GENERATOR MATRIX FOR $\mathcal{C}^{\perp}$

$$G H^T = \underset{k \times (n-k)}{0}$$

H CONTROL MATRIX FOR $\mathcal{C}$:

FOR DECODING

$$\vec{x} \in \mathcal{C} \iff H \vec{x}^T = \vec{0}$$

$H \vec{r}^T \longleftarrow$ SYNDROME OF THE RECEIVED WORD $\vec{r}$

QUANTUM SYSTEM: WHATEVER PHYSICAL PHENOMENON

Ex POLARIZATION DIRECTION OF VIBRATION OF LIGHT (ORTHOGONAL TO THE PATH OF LIGHT)

STATE OF A QUANTUM SYSTEM IS REPRESENTED BY A COMPLEX VECTOR OF LENGTH 1 IN A COMPLEX LINEAR SPACE

DIMENSION OF THE LINEAR SPACE

- USUALLY INFINITE
- FOR US: FINITE

BRA-KET NOTATION

$|\psi\rangle$ COLUMN VECTOR

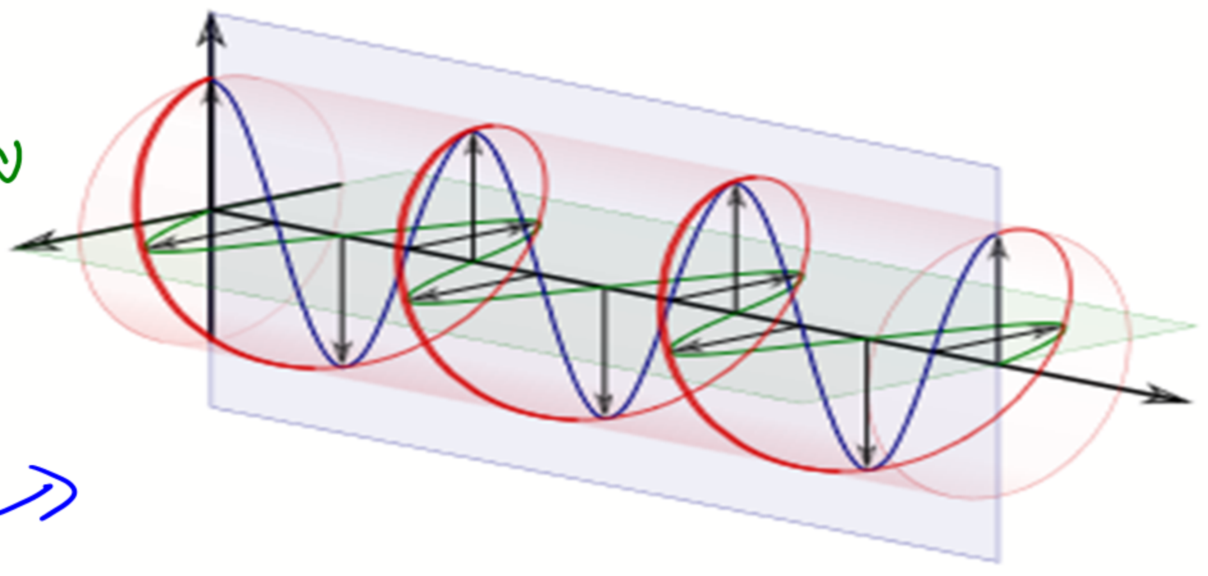
$\langle\psi|$ CONJUGATE TRANSPOSE $\left(\langle\psi| = \overline{|\psi\rangle}^{T} = |\psi\rangle^{*} \right)$

Ex $|-\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|\,|\,\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$|/\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $|\backslash\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$

$|-\rangle$

$|\,|\,\rangle$

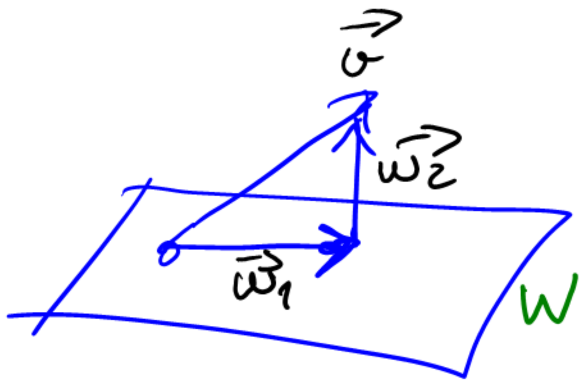


$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$

CIRCULAR POLARIZATION

PROJECTION ONTO A SUBSPACE

$$\vec{v} = \underset{\underset{W}{\cap}}{\vec{w}_1} + \underset{\underset{W^\perp}{\cap}}{\vec{w}_2}$$



$|\psi_1\rangle, \ldots, |\psi_m\rangle$ ORTHONORMAL BASIS OF W

$$P_W = |\psi_1\rangle\langle\psi_1| + \cdots + |\psi_m\rangle\langle\psi_m| \quad \text{(MATRIX)}$$

$$\vec{w}_1 = P_W(\vec{v}) = P_W|\vec{v}\rangle = |\vec{w}_1\rangle$$

SPECTRAL DECOMPOSITION:

M HERMITIAN MATRIX: $M = \overline{M}^T = M^*$

$$M = \sum_{i=1} \lambda_i P_i$$

λ_i: EIGENVALUE

P_i: PROJECTION ONTO W_i EIGENSPACE ASSOCIATED TO λ_i

- COMPUTE λ_i, W_i (EIGENVALUES, EIGENSPACES)
- COMPUTE ORTHONORMAL BASIS $\{|\varphi_{i_1}\rangle, \dots, |\varphi_{i_m}\rangle\}$ OF W_i
- $P_i = \sum_{k=1}^{m} |\varphi_{i_k}\rangle\langle\varphi_{i_k}|$

EXAMPLE SPECTRAL DECOMPOSITION

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

EIGENVALUES : $+1 \quad -1$

EIGENVECTORS : $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$$Z = +1 \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} \right) + (-1) \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} \right) =$$

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

EXAMPLE: SPECTRAL DECOMPOSITION

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

EIGENVALUES: $+1 \quad -1$

EIGENVECTORS: $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$

$$X = 1\left(\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \end{pmatrix}\right) + (-1)\left(\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \end{pmatrix}\right) =$$

$$= +1\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} + (-1)\begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix}$$

MEASUREMENT

$\mathcal{H}$: LINEAR SPACE ASSOCIATED WITH A QUANTUM SYSTEM

AN OBVERVABLE A: AN HERMITIAN MATRIX ON $\mathcal{H}$

RESULTS OF MEASURING THE OBSERVABLE A:

$$\boxed{\text{EIGENVALUES OF } A}$$

- WE CANNOT PREDICT MEASUMENT OUTCOME
- BUT WE CAN CALCULATE THE PROBABILITY OF A MEASURENT OUTCOME

PROBABILITY OF GETTING A MEASUREMENT OUTCOME

- $|\psi\rangle$: QUANTUM SYSTEM STATE
- OBSERVABLE A, WITH EIGENVALUES $\lambda_1, \dots, \lambda_n$

$$A = \lambda_1 P_1 + \cdots + \lambda_n P_n$$ (SPECTRAL DECOMPOSITION)

- PROBABILITY OF GETTING λ_i AS THE MEASUREMENT OUTCOME IS $\| P_i |\psi\rangle \|^2$

EX

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = 1 \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}}_{= P_1} - 1 \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}_{= P_2}$$

$$|\psi\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$P_1 |\psi\rangle = |\psi\rangle \Rightarrow$ PROBABILITY GETTING $+1$ IS 1

$P_2 |\psi\rangle = 0 \Rightarrow$ PROBABILITY GETTING -1 IS 0

$$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \qquad P_1|\psi\rangle = \begin{pmatrix} a \\ 0 \end{pmatrix} \Rightarrow \text{PROBABILITY GETTING } +1 \text{ IS } |a|^2$$

$$|a|^2 + |b|^2 = 1 \qquad P_2|\psi\rangle = \begin{pmatrix} 0 \\ b \end{pmatrix} \Rightarrow \text{PROBABILITY GETTING } -1 \text{ IS } |b|^2$$

Ex

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = 1 \underbrace{\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}}_{= P_1} - 1 \underbrace{\begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix}}_{= P_2}$$

$$|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$$

$$\| P_1 |\psi\rangle \|^2 = \left\| \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \right\|^2 = \left\| \frac{1}{2\sqrt{2}} \begin{pmatrix} 1+i \\ 1+i \end{pmatrix} \right\|^2 =$$

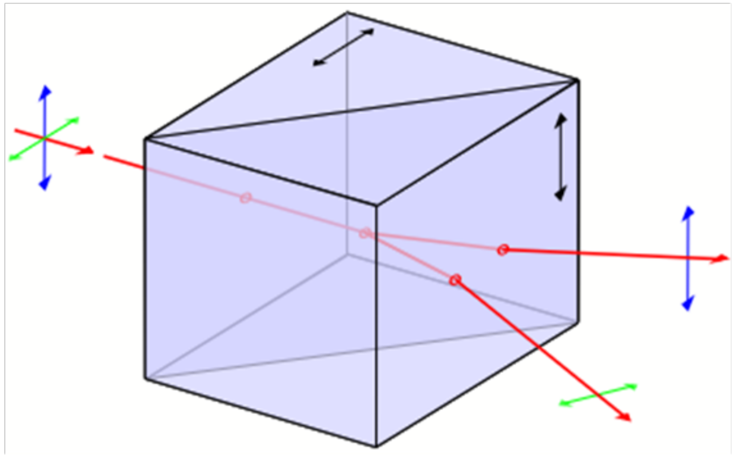
$$= \left(\frac{1}{2\sqrt{2}}\right)^2 (1+1+1+1) = \frac{4}{8} = \frac{1}{2}$$

$$\| P_2 |\psi\rangle \|^2 = \dots\dots = 1/2$$

NONDESTRUCTIVE MEASUREMENT

- SLIT: THE PHOTON CAN BE ABSORBED

- PRISM OF CALCITE



STATE AFTER NONDESTRUCTIVE MEASUREMENT

AFTER GETTING OUTCOME λ_i, THE STATE BECOMES

$$\frac{P_i |\psi\rangle}{\| P_i |\psi\rangle \|}$$

Ex

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = 1 \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}}_{"P_1} + (-1) \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}_{"P_2}$$

$$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$$

$$|a|^2 + |b|^2 = 1$$

$$\frac{P_1 |\psi\rangle}{\| P_1 |\psi\rangle \|} = \frac{\begin{pmatrix} a \\ 0 \end{pmatrix}}{|a|} = \begin{pmatrix} a/|a| \\ 0 \end{pmatrix} \sim \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |-\rangle$$

(PROBABILITY $|a|^2$)

$$\frac{P_2 |\psi\rangle}{\| P_2 |\psi\rangle \|} = \frac{\begin{pmatrix} 0 \\ b \end{pmatrix}}{|b|} = \begin{pmatrix} 0 \\ b/|b| \end{pmatrix} \sim \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

(PROBABILITY $|b|^2$)

MANIPULATION OF A QUANTUM SYSTEM WITHOUT STRACTING INFORMATION IS REPRESENTED BY A UNITARY MATRIX U $(UU^* = Id)$

Ex $|-\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$X|-\rangle = |1\rangle$

$X|1\rangle = |-\rangle$

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

$Z|1\rangle = -|1\rangle$ (PHYSICALLY EQUIVALENT TO $|1\rangle$)

TENSOR PRODUCT

V, W LINEAR SPACES

$V \otimes W$: LINEAR SPACE SPANNED BY

$$\{ |\psi\rangle \otimes |\psi\rangle \mid |\varphi\rangle \in V, |\psi\rangle \in W \}$$

$$\dim V \otimes W = \dim V \times \dim W$$

$$(\dim V \times W = \dim V + \dim W)$$

A $m \times n$ MATRIX

B $p \times q$ MATRIX

$mp \times nq$ MATRIX

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}$$

COMPOSITE SYSTEM

$\mathcal{H}_1$: A QUANTUM SYSTEM

$\mathcal{H}_2$: A QUANTUM SYSTEM

THE QUANTUM SYSTEM CONSISTING OF SYSTEM 1 AND 2 IS REPRESENTED BY $\mathcal{H}_1 \otimes \mathcal{H}_2$

APPLIYING U_1 TO $\mathcal{H}_1$ $\equiv$ APLLIYING $U_1 \otimes I$ TO $\mathcal{H}_1 \otimes \mathcal{H}_2$

MEASURING A_1 OF $\mathcal{H}_1$ $\equiv$ MEASURING $A_1 \otimes I$ OF $\mathcal{H}_1 \otimes \mathcal{H}_2$

ENTANGLEMENT STATE

A STATE THAT CANNOT BE WRITTEN AS

$$|\varphi\rangle \otimes |\psi\rangle \quad \text{FOR ANY } \varphi \in V,\ \psi \in W$$

$$|\vec{v}_1\rangle \otimes |\vec{w}_1\rangle + |\vec{v}_2\rangle \otimes |\vec{w}_2\rangle$$

SPECTRAL DECOMPOSITION OF $A \otimes B$

$$A = \lambda_1 P_1 + \dots + \lambda_m P_m$$

$$B = \eta_1 Q_1 + \dots + \eta_n Q_n$$

$$A \otimes B = \sum_{i=1}^{m} \sum_{j=1}^{n} \underbrace{\lambda_i \eta_j}_{\text{EIGENVALUES OF } A \otimes B} P_i \otimes Q_j$$

NO CLONING THEOREM

IMAGINE THAT THERE EXISTS A UNITARY OPERATOR U FOR AN ARBITRARY STATE $|\varphi\rangle$ AND FIXED STATE $|\psi\rangle$

$$U(|\varphi\rangle \otimes |\psi\rangle) = |\varphi\rangle \otimes |\varphi\rangle$$

BLANK PAPER

↯ U IS NOT LINEAR

$$U((|\varphi_1\rangle + |\varphi_2\rangle) \otimes |\psi\rangle) \overset{\text{DEF } U}{=} (|\varphi_1\rangle + |\varphi_2\rangle) \otimes (|\varphi_1\rangle + |\varphi_2\rangle)$$

$\|$ LINEARITY WOULD IMPLY

$$U(|\varphi_1\rangle \otimes |\psi\rangle) + U(|\varphi_2\rangle \otimes |\psi\rangle) \underset{\text{DEF } U}{=} |\varphi_1\rangle \otimes |\varphi_1\rangle + |\varphi_2\rangle \otimes |\varphi_2\rangle$$

$\#$

A TWO DIMENSIONAL QUANTUM SYSTEM IS SAID TO BE A QUBIT

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

NOTATION:

$$|\varphi\rangle \otimes |\psi\rangle = |\varphi\rangle |\psi\rangle = |\varphi\psi\rangle$$

WE WANT TO SEND A QUBIT $\alpha|0\rangle+\beta|1\rangle$

ERROR MODEL:

- EACH QBIT TRANSMITED CAN BE MULTIPLIED BY $X=\begin{pmatrix}0&1\\1&0\end{pmatrix}$ (OR RECEIVED WITH NO CHANGE)
- ERRORS ON EACH QBIT ARE STATISTICALLY INDEPENDENT

ENCODER: $\alpha|0\rangle+\beta|1\rangle \longmapsto \alpha|000\rangle+\beta|111\rangle$

- PREPARE $|00\rangle$ AND ATTACH IT TO $\alpha|0\rangle+\beta|1\rangle$ TO GET $(\alpha|0\rangle+\beta|1\rangle)|00\rangle=\alpha|000\rangle+\beta|100\rangle$
- APLY UNITARY MATRIX $|000\rangle\longmapsto|000\rangle$
  $|100\rangle\longmapsto|111\rangle$

DECODER

1) MEASURE $Z \otimes Z \otimes I$ AND $I \otimes Z \otimes Z$

NOTE: • ORDER DOES NOT MATTER

• THE STATE BELONGS TO THE EIGENSPACE OF THE MEASUREMENT. HENCE WE DO NOT MODIFY IT.

2) "SYNDROME" $\rightarrow$ APPLY UNITARY MATRIX

$Z \otimes Z \otimes I$	$I \otimes Z \otimes Z$	"SYNDROME"
$+1$	$+1$	NOTHING
$+1$	-1	$I \otimes I \otimes X$
-1	$+1$	$X \otimes I \otimes I$
-1	-1	$I \otimes X \otimes I$

3) INVERSE OF ENCODING

EXAMPLE

ERROR $X\otimes I\otimes I$

$$\alpha|000\rangle+\beta|111\rangle \longmapsto \alpha|100\rangle+\beta|011\rangle$$

$Z\otimes Z\otimes I\,(\alpha|1\underbrace{00}\rangle+\beta|\underbrace{01}1\rangle)$ OUTCOME -1 PROBAB. 1

$I\otimes Z\otimes Z\,(\alpha|100\rangle+\beta|011\rangle)$ OUTCOME $+1$ PROBAB. 1

DECODING: APPLY $X\otimes I\otimes I$ TO $\alpha|100\rangle+\beta|011\rangle$

TO GET $\alpha|000\rangle+\beta|111\rangle$

EX $Z\otimes Z=+1\underbrace{(|00\rangle\langle 00|+|11\rangle\langle 11|)}_{P_{+1}}+(-1)\underbrace{(|10\rangle\langle 10|+|01\rangle\langle 01|)}_{P_{-1}}$

$$P_{-1}(\alpha\underbrace{|10\rangle}+\beta\underbrace{|01\rangle})=\alpha(|10\rangle\underbrace{\langle 10|10\rangle}_{=1}+|01\rangle\underbrace{\langle 01|10\rangle}_{=0})+$$

$$\beta(|10\rangle\underbrace{\langle 10|01\rangle}_{=0}+|01\rangle\underbrace{\langle 01|01\rangle}_{=1})$$

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

Z ERROR ?

IF $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ ERROR OCCURS AT ONE QBIT :

$$\alpha|000\rangle + \beta|111\rangle \longmapsto \alpha|000\rangle - \beta|111\rangle$$

MEASUREMENT OUTCOME OF $Z \otimes Z \otimes I = +1$ PROBABILITY 1

MEASUREMENT OUTCOME OF $I \otimes Z \otimes Z = +1$ PROBABILITY 1

Ex $$Z \otimes Z \otimes I = +1 \underbrace{\left(|00\rangle\langle 00| + |11\rangle\langle 11|\right)}_{= P_{+1}} \otimes I + (-1) \underbrace{\left(|10\rangle\langle 10| + |01\rangle\langle 01|\right)}_{= P_{-1}} \otimes I$$

$$(P_{+1} \otimes I)\left(\alpha|000\rangle \pm \beta|111\rangle\right) = |00\rangle\langle 00| \otimes I \left(\alpha|000\rangle \pm \beta|111\rangle\right) + |11\rangle\langle 11| \otimes I \left(\alpha|000\rangle \pm \beta|111\rangle\right) =$$

$$\alpha|000\rangle \pm \beta|111\rangle$$

THE SHOR CODE

- ENCODES 1 QBIT IN 9 QBITS
- DECODES AN ARBITRARY ERROR IN 1 QBIT

$$|0\rangle \longmapsto \frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$$

$$|1\rangle \longmapsto \frac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$$

CORRECTING X ERROR

NOTE: EACH TRIPLE OF QBITS IS THE SAME AS THE PREVIOUS ERROR CORRECTING CODE

$X_i = X$ ACTING ON i-TH BIT

$Z_i = Z$ ACTING ON i-TH BIT

WE MEASURE

$$Z_1 \otimes Z_2 \qquad Z_2 \otimes Z_3$$

$$Z_4 \otimes Z_5 \qquad Z_5 \otimes Z_6$$

$$Z_7 \otimes Z_8 \qquad Z_8 \otimes Z_9$$

CORRECTING Z ERROR

WE MEASURE

$$\begin{cases} X_1 \otimes X_2 \otimes \cdots \otimes X_6 \\ X_4 \otimes X_5 \otimes \cdots \otimes X_9 \end{cases}$$

- $(|000\rangle \pm |111\rangle)(|000\rangle \pm |111\rangle) \in$ • EIGENSPACE OF $+1$

  IF BOTH "$\pm$" ARE THE SAME

- OTHERWISE $\in$ EIGENSPACE OF -1

Z ERRORS CHANGE THE SIGN $\pm$:

$$\begin{matrix} Z_1 \otimes I \otimes I \\ I \otimes Z_2 \otimes I \\ I \otimes I \otimes Z_3 \end{matrix} \; (|000\rangle \pm |111\rangle) = |000\rangle \mp |111\rangle$$

SYNDROME:

OBSERVABLE				
$X_1 \otimes \cdots \otimes X_6$	+1	−1	−1	+1
$X_4 \otimes \cdots \otimes X_9$	+1	+1	−1	−1
APPLY	NOTHING NO ERROR	Z_1 OR Z_2 OR Z_3	Z_4 OR Z_5 OR Z_6	Z_7 OR Z_8 OR Z_9

CORRECTION OF XZ ERROR

BOTH
- X ERROR CORRECTION
- Z ERROR CORRECTION

CORRECTION OF AN ARBITRARY ERROR

U 2X2 UNITARY MATRIX "NOISE"

$$U = a_I I + a_X X + a_Z Z + a_{XZ} XZ$$

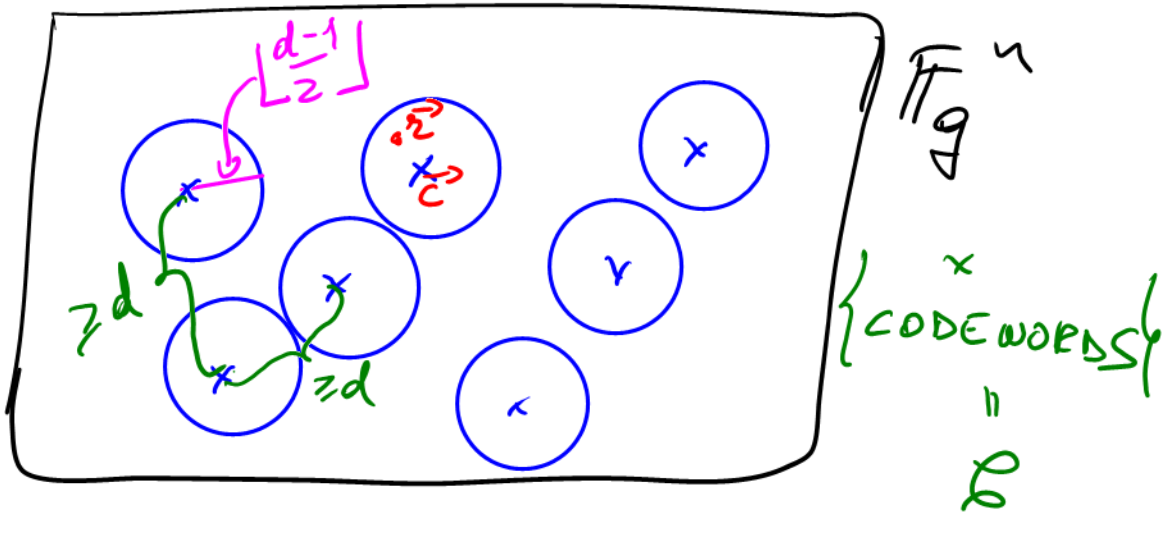
$$\left.\begin{aligned}|\psi\rangle = \alpha \frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}} + \\ \beta \frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}\end{aligned}\right\} \text{BEFORE ERROR}$$

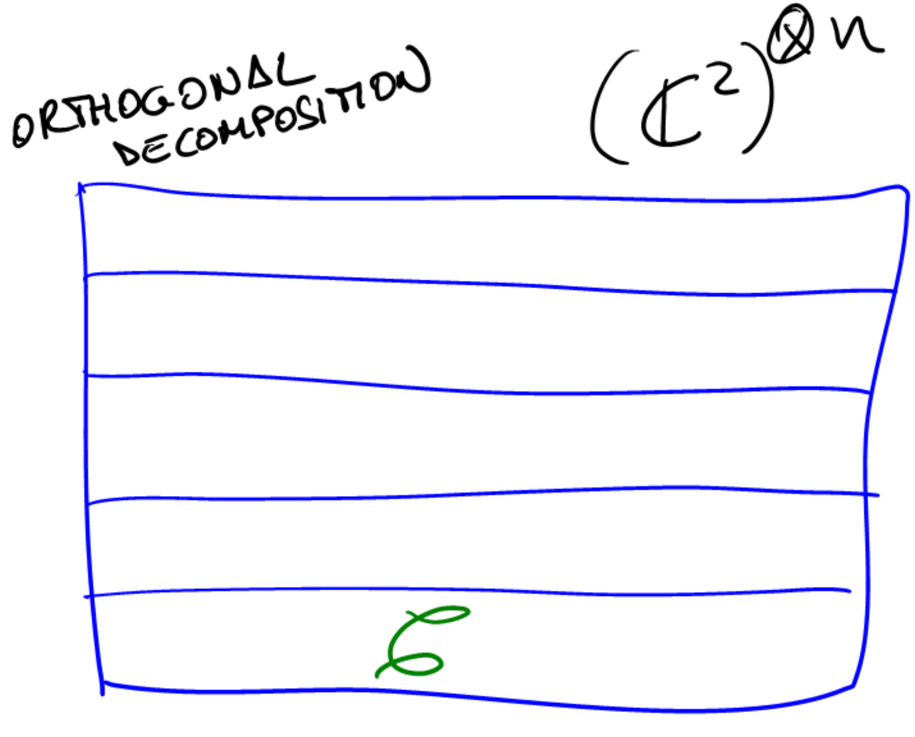
AFTER ERROR:

$$U \otimes I^{\otimes 8} |\psi\rangle = a_I I \otimes I^{\otimes 8} |\psi\rangle + a_X X \otimes I^{\otimes 8} |\psi\rangle + a_Z Z \otimes I^{\otimes 8} |\psi\rangle + a_{XZ} XZ \otimes I^{\otimes 8} |\psi\rangle$$

- THE STATE AFTER A SINGLE X, Z, XZ ERROR IS AN EIGENSTATE OF THE OBSERVABLE FOR ERROR CORRECTION

- EACH TERM IN PREVIOUS EXPRESSION BELONGS TO DIFFERENT EIGENVALUES. AFTER MEASUREMENT ONLY ONE TERM REMAINS. AND THE ERROR IS I, X, Z OR XZ





CSS (Calderbank-Shor-Steane) construction

Th: Let $\mathcal{C}_1, \mathcal{C}_2$ two linear codes with parameters $[n, k_1, d_1]_q$, $[n, k_2, d_2]_q$ such that $\mathcal{C}_2^\perp \subset \mathcal{C}_1$

Then there exists an $[[n, k_1+k_2-n, d]]_q$ quantum stabilizer code with

$[[9,1,3]]_2$

$$d = \min\{ w(c) \mid c \in (C_1 \setminus C_2^\perp) \cup (C_2 \setminus C_1^\perp) \}$$

Corollary: Let $\mathcal{C}$ a linear code $[n, k, d]$ with

$\mathcal{C}^\perp \subset \mathcal{C}$ then there exists a

$[[n, 2k-n, \geq d]]_q$ quantum stabilizer code

ONE CAN IMPROVE THE PREVIOUS RESULT WITH HERMITIAN LINEAR PRODUCT

$$\vec{x} \bullet_h \vec{y} = \sum_{i=1}^{n} x_i y_i^q , \quad \vec{x}, \vec{y} \in \mathbb{F}_{q^2}$$

Th: $\mathcal{C}\ [n,k,d]_{q^2}$ / $\mathcal{C}^{\perp_h} \subset \mathcal{C} \Rightarrow$

$$\exists\ [[n, 2k-n, \geq d]]_q$$