QUANTUM ERROR CORRECTION

K. R. PARTHASARATHY

INDIAN STATISTICAL INSTITUTE
DELHI CENTRE

krp@isid.ac.in

$\mathcal{H}$ Complex Hilbert space of finite dimension

$\mathcal{B}(\mathcal{H})$ Algebra of all operators on $\mathcal{H}$ with involution $A \to A^\dagger$

$\mathcal{N} \subset \mathcal{B}(\mathcal{H})$ subspace of 'small' dimension called <u>NOISE</u> or <u>ERROR</u> subspace

ρ <u>input state</u> from $\mathcal{H}$

$\hat{\rho}$ <u>output state</u> from $\mathcal{H}$

$$\hat{\rho} = \frac{\sum_j N_j \rho N_j^\dagger}{\mathrm{Tr}\, \rho \sum N_j^\dagger N_j} \qquad N_j \in \mathcal{N}, \ \underline{\text{unknown}} \qquad (1)$$

Recovery or Decoding operation $\mathcal{R}$:

$$\mathcal{R} = \{ R_1, R_2, \dots \}, \quad \sum_j R_j^\dagger R_j = I$$

$$\mathcal{R}(\hat{\rho}) = \sum_j R_j \hat{\rho} R_j^\dagger . \tag{2}$$

PROBLEM Given $\mathcal{N}$ find a subspace $\mathcal{C} \subset \mathcal{H}$ and a recovery operation $\mathcal{R}$ so that

$$\mathcal{R}(\hat{\rho}) = \rho \quad \text{if} \quad (\text{Supp}\, \rho) \subset \mathcal{C},$$

$$\text{i.e.,} \quad \rho |\psi\rangle = 0 \quad \forall \psi \in \mathcal{C}^\perp$$

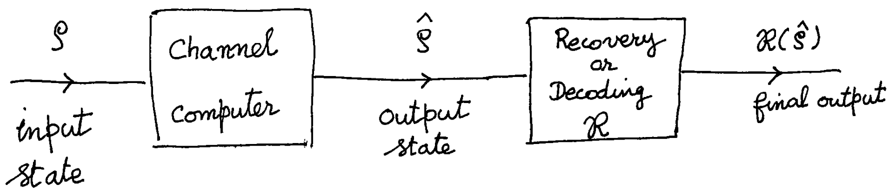
$\hat{\rho}$, $\mathcal{R}$ as in (1), (2).

$(\mathcal{C}, \mathcal{R})$ $\mathcal{N}$- correcting quantum code (Q.C.)

(Error correcting quantum code)

Construct $\mathcal{N}$- correcting Q.C. so that dim $\mathcal{C}$ is as large as possible and use states from $\mathcal{C}$ for error-free communication.

SEE PICTURE NEXT PAGE.



$$\sum_j R_j N |\psi\rangle\langle\psi| N^\dagger R_j^\dagger = \|N\psi\|^2 \, |\psi\rangle\langle\psi| \qquad \forall \; |\psi\rangle \in \mathcal{C}, \; N \in \mathcal{N} \tag{3}$$

<u>PROPOSITION 1</u> $(\mathcal{C}, \mathcal{R})$ is an $\mathcal{N}$-correcting Q.C. iff

$$R_j N |\psi\rangle = \lambda_j(N) |\psi\rangle \quad \forall \; \psi \in \mathcal{C}, \; N \in \mathcal{N}, j$$

where $\lambda_j(N)$ is a scalar.

P = Projection on $\mathcal{C} \subset \mathcal{H}$

If $\mathcal{C}$ admits a recovering operation $\mathcal{R}$ so that $(\mathcal{C}, \mathcal{R})$ is an $\mathcal{N}$-correcting quantum code we say that the projection P is an $\mathcal{N}$-correcting quantum code.

<u>Theorem 2</u> (Knill and Laflamme Phys. Rev A. 1997)

A Projection P in $\mathcal{H}$ is an $\mathcal{N}$-correcting quantum code iff

$$P N_1^\dagger N_2 P = \lambda(N_1^\dagger N_2) P \quad \forall \quad N_1, N_2 \in \mathcal{N}$$

where $\lambda(N_1^\dagger N_2)$ is a scalar.

$$\langle N_1 | N_2 \rangle \triangleq \lambda(N_1^\dagger N_2)$$ Pre Hilbert Scalar product in $\mathcal{N}$

$\mathcal{N}_0 = \{ N | \langle N | N \rangle = 0 \}$

$\mathcal{N}/\mathcal{N}_0$ quotient space $[N] = N + \mathcal{N}_0$

$\langle [N_1] | [N_2] \rangle = \langle N_1 | N_2 \rangle = \lambda(N_1^\dagger N_2)$ makes

$\mathcal{N}/\mathcal{N}_0$ a Hilbert space $= \tilde{\mathcal{N}}$

Choose an orthonormal basis here

$[N_1], [N_2], \ldots, [N_k]$

so that $\langle [N_i] | [N_j] \rangle = \delta_{ij}$.

Put

$$N_i P N_i^\dagger \triangleq P_i$$

$$P_i P_j = \delta_{ij} P_j \qquad Q \triangleq I - \sum_{i=1}^{k} P_i .$$

$P_1 + \cdots + P_k + Q = I$ (Resolution of I into orthogonal projections)

Define

$$R_j = \begin{cases} P N_j^{\dagger} & 1 \leq j \leq k, \\ Q & j = k+1 \end{cases}$$

Then $(\text{Range } P, \ \mathcal{R})$, $\mathcal{R} = (R_1, R_2, \dots)$

is an $\mathcal{N}$-correcting Q.C.

Define $(k+1) \times (k+1)$ block $\mathcal{H}$-operator matrix U with i-th row

$$N_1 P N_i^{\dagger}, \ N_2 P N_i^{\dagger}, \dots N_{k+1-i} P N_i^{\dagger}, \ Q, \ N_{k+3-i} P N_i^{\dagger} \dots N_k P N_i^{\dagger}, \ N_{k+2-i} P N_i^{\dagger}$$

if $1 \leq i \leq k$

$$Q, \ N_2 P N_k^{\dagger}, \ N_3 P N_{k-1}^{\dagger}, \dots \ N_k P N_2^{\dagger} \ N_1 P_{\flat} N_1^{\dagger}$$

if $i = k+1$

PROPOSITION 3 U is a unitary operator in $\mathcal{H} \otimes (\tilde{N} \oplus \mathbb{C})$ and selfadjoint.

Furthermore $U^2 = I$.

(U is a reflection)

Let $I \in \mathcal{N}$. Choose $N_1 = I$.

In the auxiliary Hilbert space $\tilde{\mathcal{N}} \oplus \mathbb{C}$ put

$$|\Omega\rangle = |[I]\rangle$$

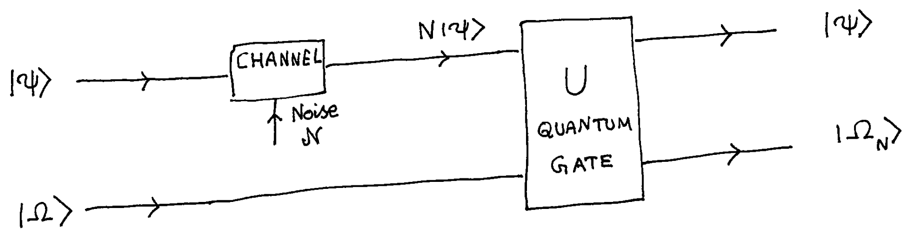
Recall $\mathcal{C}$ = Range P. Then

$$U\,|\psi\rangle|\Omega\rangle = \begin{bmatrix} P|\psi\rangle \\ PN_2^\dagger|\psi\rangle \\ \vdots \\ PN_k^\dagger|\psi\rangle \\ Q|\psi\rangle \end{bmatrix} \quad \forall\ \psi \in H$$

$$U\,N|\psi\rangle|\Omega\rangle = |\psi\rangle|\Omega_N\rangle \quad \forall\ \psi \in \mathcal{C}$$

$$|\Omega_N\rangle = [\,\lambda(N),\ \lambda(N_2^\dagger N),\ \ldots,\ \lambda(N_k^\dagger N),\ 0\,]^T$$

$$\mathcal{R}(\rho) = \mathrm{Tr}_2\ U(\rho \otimes |\Omega\rangle\langle\Omega|)\,U^\dagger \quad \forall\ \rho \text{ in } \mathcal{H}$$



$|\psi\rangle \in \mathcal{C}$.

Noise - free communication of states.

<u>A general picture</u>

The Standard Model of Noise

$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$

Hilbert space of a composite system made of n component systems.

$1 \leq t \leq n$

$\mathcal{N}_t \subset \mathcal{B}(\mathcal{H})$ Subspace spanned by operators of the form $X_1 \otimes X_2 \otimes \cdots \otimes X_n$ where at most t of the operators $X_1, X_2, \ldots, X_n$ are different from identity.

Any element of $\mathcal{N}_t$ is said to have <u>weight</u> $\leq t$.

Any element of $\mathcal{N}_t \setminus \mathcal{N}_{t-1}$ is said to have <u>weight</u> t

An $\mathcal{N}_t$- correcting quantum code is called a <u>t - error correcting quantum code</u>.

If $\mathcal{C}$ is such a code $\dim \mathcal{C}$ = <u>size of the code</u>.

<u>Problem</u>: If $\dim \mathcal{H}_j = d_j$, $1 \leq j \leq n$ what is the maximum possible size for a t - error correcting code? n = <u>length of the code</u>

PROPOSITION - 4

In $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3 \otimes \mathcal{H}_4$ there does not exist a single error correcting quantum code of size 2.

(Proof : See KRP PHYSICS NEWS oct 2010)

PROPOSITION - 5 In $\mathcal{H}_1^{\otimes 5}$ there exists a single error correcting quantum code of size = dim $\mathcal{H}_1$.

When $\mathcal{H}_1 = \mathbb{C}^2$ (one qubit Hilbert space a size 2 single error correcting code is spanned by

$$
\begin{aligned}
|\psi_0\rangle = \frac{1}{4}\{ & |00000\rangle + |11000\rangle + |01100\rangle + |00110\rangle \\
& + |00011\rangle + |10001\rangle \\
& - (|10100\rangle + |01010\rangle + |00101\rangle + |10010\rangle + |01001\rangle \\
& + |10100\rangle) \\
& - (|11110\rangle + |01111\rangle + |10111\rangle + |11011\rangle \\
& + |11101\rangle)
\end{aligned}
$$

$|\psi_1\rangle$ = (Interchange 0 and 1 in $|\psi_0\rangle$).

This was first constructed by Laflamme by computer search. For PROPOSITION 5 there is a group-theoretic construction generalizing the 1-qubit example.

Remark Let $|\psi\rangle = a|\psi_0\rangle + b|\psi_1\rangle$, $|a|^2 + |b|^2 = 1$. Then

$$\mathrm{Tr}_3 |\psi\rangle\langle\psi| = \frac{1}{4} I$$

where Tr_3 is relative trace over any 3 copies of $\mathbb{C}^2$ in $(\mathbb{C}^2)^{\otimes 5}$. i.e., $|\psi\rangle$ is maximally entangled