QUANTUM INFORMATION —- THE NO-HIDING THEOREM

Arun K Pati

akpati@iopb.res.in

Instititute of Physics, Bhubaneswar-751005, Orissa, INDIA

and

Th. P. D, BARC, Mumbai-400085, India

Quantum Information (QI)

- Exploits basic features of quantum theory in information processing.
- Fundamental new insight into nature of quantum world and physical processes.
- QI technology utilizes resources that are not available in classical world.
- Recent developments: Quantum computing, Quantum teleportation, Dense Coding, Remote state preparation, Quantum communications, Quantum cryptography and many more.

Classical and Quantum Information

- Classical bit remains in either 0 or 1.
- Quantum bit (qubit) can not only remain in 0 or 1, but also in 0 and 1.
- Any general two-state quantum system is a qubit:

$$|\psi(\theta,\phi)\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle.$$

- Quantum theory allows new ways of storing and processing information which are not there in the classical world.

Quantum Theory

- System is described by a state vector $|\psi\rangle \in \mathcal{H}$.
- Physical observables are linear Hermitian operators.
- Quantum evolution is linear. Closed quantum systems evolve unitarily, i.e., $|\psi\rangle \rightarrow |\psi'\rangle = U|\psi\rangle$. Unitary evolution preserves purity of a state.
- Measurement disturbs the state.

If we know the outcome: $|\psi\rangle = \sum_n c_n|\psi_n\rangle \rightarrow |\psi_n\rangle$ with probability $|c_n|^2$.

If we do not know the outcome:

$|\psi\rangle\langle\psi| \rightarrow \sum_n |c_n|^2|\psi_n\rangle\langle\psi_n|$ —— a mixed state.

Quantum Theory ....

- State space of a composite system is tensor product of individual Hilbert spaces $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$.
- If state of the composite system cannot be written as $|\Psi\rangle_{12} = |\psi\rangle_1 \otimes |\phi\rangle_2$, then it is an entangled state.
- A general entangled state $|\Psi\rangle_{12} = \sum_{nm=1}^{NM} C_{nm} |\psi_n\rangle_1 \otimes |\phi_m\rangle_2$.
- Schmidt decomposition theorem: Any pure bipartite entangled state can be written as $|\Psi\rangle_{12} = \sum_{i=1}^{N} \sqrt{p_i} |a_i\rangle_1 \otimes |b_i\rangle_2$.
- State of individual system can be obtained by partial trace: $\rho_1 = \mathrm{tr}_2(|\Psi\rangle_{1212}\langle\Psi|)$ and $\rho_2 = \mathrm{tr}_1(|\Psi\rangle_{1212}\langle\Psi|)$.

Quantum Theory ....

- Open system is described by mixed state $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. ρ is positive, $\mathrm{tr}\rho = 1$ and $\rho^2 \neq \rho$.
- Purification: Any mixed state can be a part of a composite system which is in a pure entangled state.
- General quantum evolution is a completely positive map:

$$\rho \rightarrow \mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger,$$

where E_i's are Kraus operators and $\sum_i E_i^\dagger E_i = 1$.

- $\mathcal{E}$ can be represented as a unitary evolution in an enlarged Hilbert space.

Quantum Information

- State vector $|\psi\rangle$ carries both quantum and classical information.

- Quantum state contains potentially a vast amount information which is inaccessible to an external observer. This *inaccessible information* is quantum information.

- The amount of information we can extract from a quantum state via measurement is the accessible information and this is classical information.

- Given a single quantum in an unknown state we cannot determine it.

• Quantum Information differs from classical information in many ways. Some fundamental differences are:

- No-Cloning Theorem: We cannot make copy of an unknown quantum state (Wootter-Zurek, Nature 1982, Dieks PLA 1982).

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

- No-Flipping Theorem: We cannot flip an unknown qubit (Buzek, Hillery, Werner PRA 1999, Pati PRA 1999).

$$|\psi\rangle \rightarrow |\bar{\psi}\rangle$$

- No-Deleting Theorem: We cannot delete an unknown quantum state against a copy (Pati-Braunstein, Nature 2000).

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

- No-Partial Erasure Theorem: We cannot erase part of the information of an unknown quantum state (Pati-Sanders, PLA 2006).

$$|\psi(\theta,\phi)\rangle \rightarrow |\psi(\theta)\rangle$$

These limitations tell you what we can and cannot do with quantum information.

Hiding Classical Information

- Classical information can be hidden in two ways: Moving the original system or/and by encrypting the message.

- Vernam Cipher: Alice encodes a message M using a random n-bit key K, i.e., $C = M \oplus K$. Original message can be retrieved by receiver (say Bob) using $C \oplus K = M$, where $\oplus$ is addition modulo 2.

- Encoded bit string contains no information of the original message (Shannon, 1949).

- Where does the information reside? Neither in the encoded message nor in the key, but in the correlations between these two strings.

- Quantum analogue: Can we encode a quantum state into the correlations between two subsystems, such that subsystems have no information?

- Impossible for any *pure-state* encoding. For e.g. $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha(|00\rangle - |11\rangle) + i\beta(|01\rangle + |10\rangle)$. Individual subsyetms have some information about α and β.

- That this holds generally is particularly surprising.

Hiding Quantum Information

• Can we hide quantum information in same way like classical information?

No. If the original information is missing then it must move to somewhere else and it cannot be hidden in the correlations between a pair of systems.

This we call the 'no-hiding theorem' (Braunstein and Pati, PRL, 2007).

• This has many applications:

1. Randomization.
2. Quantum Teleportation.
3. Process involving Thermalisation– a Generalized version of Landauer's erasure.
4. Black hole Information loss paradox.

Perfect hiding processes

- Hiding process maps an arbitrary state to a fixed state

$$|\psi\rangle\langle\psi| = \rho \rightarrow \sigma.$$

- Unitary evolution cannot transform this but a general quantum operation can.

- Take an arbitrary input state ρ_I and encodes it into a larger Hilbert space in a unitary manner: $|\psi\rangle_I \rightarrow |\Psi\rangle_{OA}$. If $\sigma_O = \mathrm{tr}_A(|\Psi\rangle_{OA}\langle\Psi|)$ is independent of the input state, then it is a hiding process.
- The remainder of the encoded Hilbert space is ancilla A which itself could be a composite system.

The No-Hiding Theorem

- Theorem: *Let* $|\psi\rangle_I \rightarrow |\Psi\rangle_{OA}$ *such that* $|\psi\rangle_{II}\langle\psi| = \rho_I \rightarrow \sigma_O$ *with* σ *fixed for all* ρ*. Then the missing information is wholly encoded in the remainder of Hilbert space with no information stored in the correlations between the two subsystems.*

- Quantum mechanics allows only one way to completely hide an arbitrary quantum state.

- This is robust to imperfections. As more of the original state becomes hidden, it smoothly becomes more accessible in the remainder of Hilbert space.

• *Proof:* For this process to be physical, it must be linear and unitary. Unitarity allows us to suitably enlarge the ancilla and that maps pure states to pure states.

• Schmidt decomposition of the final state is

$$|\psi\rangle_I \rightarrow \sum_{k=1}^{K} \sqrt{p_k}\, |k\rangle_O \otimes |A_k(\psi)\rangle_A \ ,$$

where p_k are the K non-zero eigenvalues of σ, $\{|k\rangle\}$ are its eigenvectors, and $\{|k\rangle\}$ and the ancilla states $\{|A_k\rangle\}$ are orthonormal sets.

- By linearity the ancilla will consist of an orthonormal set of states even for superposed states

$$|A_k(\alpha|\psi\rangle + \beta|\psi_\perp\rangle)\rangle = \alpha|A_k(\psi)\rangle + \beta|A_k(\psi_\perp)\rangle,$$

where $|\psi_\perp\rangle$ is orthogonal to $|\psi\rangle$.

- Inner product gives

$$\alpha^*\beta\,\langle A_l(\psi)|A_k(\psi_\perp)\rangle + \beta^*\alpha\,\langle A_l(\psi_\perp)|A_k(\psi)\rangle = 0\ .$$

For arbitrary α and β, all cross-terms must vanish.

• Given any orthonormal basis $\{|\psi_j\rangle,\ j = 1, \ldots, d\}$ spanning the input states we may now define an orthonormal set of states, $|A_{kj}\rangle \equiv |A_k(\psi_j)\rangle$. Unitarity allows us to map any orthonormal set into any other.

• We are free to write these as

$$|A_{kj}\rangle = |q_k\rangle \otimes |\psi_j\rangle$$

where $\{|q_k\rangle\}$ is an orthonormal set of K states.

• By linearity, we have
$|A_k(\psi)\rangle = |A_k(\sum_j c_j|\psi_j\rangle)\rangle = \sum_j c_j|A_k(\psi_j)\rangle$
$= \sum_j c_j|q_k\rangle \otimes |\psi_j\rangle = |q_k\rangle \otimes |\psi\rangle$

- Under this mapping the final state is

$$|\psi\rangle_I \rightarrow \sum_k \sqrt{p_k}\,|k\rangle_O \otimes (|q_k\rangle \otimes |\psi\rangle)_A.$$

- $|\psi\rangle$ can be swapped with any other state in the ancilla $\Rightarrow$ QI that is encoded globally is in fact encoded entirely within the ancilla.
- No information about $|\psi\rangle$ is encoded in system and ancilla correlations.
- *If the original information is missing it must be moved to reminder and it cannot be hidden in the correlations— the 'no-hiding theorem'.*

Imperfect hiding processes

- Imperfect hiding must allow for some imprecision in the encoding.
- To fully specify the mapping, we now need to describe its action on entangled states.
- Input subsystem I is initially entangled with an external subsystem I': $|\psi\rangle_{I'I} \equiv \sum_j \sqrt{\lambda_j}|j'\rangle_{I'}|j\rangle_I$ so that $\rho_I = \mathrm{tr}_{I'}(|\psi\rangle_{I'I}\langle\psi|) = \sum_j \lambda_j |j\rangle\langle j|$.

• Linearity and hiding map imply that a perfect hiding process has the form $|\psi\rangle_{I'I} \longrightarrow |\Psi^{\text{perfect}}\rangle_{I'OA}$

$$\equiv \sum_{jk} \sqrt{\lambda_j p_k} |j'\rangle_{I'} \otimes |k\rangle_O \otimes (|q_k\rangle \otimes |j\rangle)_A$$

• The specification we sought takes the form $\rho_{I'I} \equiv |\psi\rangle_{I'I}\ {}_{I'I}\langle\psi| \longrightarrow \rho_{I'} \otimes \sigma_O$, where $\rho_{I'}$ is the reduced state of the reference.

• An imperfect process can be described by $\rho_{I'I} \longrightarrow \rho_{I'O}$ where the output only imprecisely hides the input with $\text{tr}\,|\rho_{I'O} - \rho_{I'} \otimes \sigma_O| < \epsilon$, for some ϵ.

- Purification of $\rho_{I'O}$ is a global state $|\Psi^{\rm imperfect}\rangle$. The tensor product $\rho_{I'} \otimes \sigma_O$ is guaranteed by *any* purification which takes the form of $|\Psi^{\rm perfect}\rangle$.

- Global state of the imperfect output will strongly overlap with some global state whose form perfectly satisfies the no-hiding theorem

$$\langle \Psi^{\rm imperfect} | \, \Psi^{\rm perfect} \rangle \geq 1 - \epsilon/2 \; .$$

- Demonstrates robustness of the "no-hiding theorem" to imperfections.

Randomization

• Randomization takes an arbitrary pure state to a complete random mixture: $|\psi\rangle\langle\psi| \longrightarrow \frac{I}{d}$. A qubit can be randomized via a quantum operation $|\psi\rangle\langle\psi| \longrightarrow$

$$\frac{1}{4}[I|\psi\rangle\langle\psi|I+\sigma_x|\psi\rangle\langle\psi|\sigma_x+\sigma_y|\psi\rangle\langle\psi|\sigma_y+\sigma_z|\psi\rangle\langle\psi|\sigma_z] =$$

• Exact randomization requires an ancilla of dimension at least d^2. If we see the enlarged Hilbert space, the missing information will be in the ancilla part in accordance with the 'no-hiding' theorem.

Quantum Teleportation

- An object is destroyed at one end and recreated at a distant location using quantum entanglement and classical communication (Bennett *et al* 1993).
- Teleportation equation:

$$|\psi\rangle|\Psi^-\rangle = \frac{1}{2}\sum_{j=0}^{3}|\Psi_j\rangle_{\text{Alice}} \otimes U_j^\dagger|\psi\rangle_{\text{Bob}}.$$

- Alice measures in Bell basis $\{|\Psi_j\rangle\}$ and communicates her measurement result to Bob via a classical channel.
- Depending on classical message Bob applies U_j to recover the state. This completes the quantum teleportation.

Quantum Teleportation

- To apply the no-hiding theorem to teleportation, we require a globally quantum description or a unitary description.

- Classical message is replaced by quantum system and being send from Alice to Bob (if we allow decoherence we will get classical message, (Braunstein 1996).
- For a single qubit in an arbitrary pure state $|\psi\rangle$, the teleportation protocol reduces to

$$|\psi\rangle \rightarrow \frac{1}{2}\sum_{j=0}^{3} |\Psi_j\rangle_{\text{Alice}} \otimes |j\rangle_{\text{message}} \otimes U_j^{\dagger}|\psi\rangle_{\text{Bob}}.$$

- Each of the three subsystems is in the maximally mixed state for that space. Bob needs to undo the randomizing operations to retrieve $|\psi\rangle$.

- Our key result can be recovered by rewriting the teleportation process in terms of a bi-partite system.

- Since the reduced density matrix of Bob's subsystem contains no information about the hidden state $|\psi\rangle$, it must lie entirely in the remainder of Hilbert space (encoded within the union of the Alice and message subsystems). Same argument holds for other subsystems.

• Quantum teleportation is consistent with our result. When the original disappears it must appear somewhere else.

• Unitary variation of teleportation could serve as an experimental verification of the no-hiding theorem, where the bi-partite systems could be reconstructed separately to identify in which subsystem the qubit was encoded.

Thermalization

- The no-hiding theorem offers deep new insights into the nature of quantum information.
- Generalizes Landauer's erasure (1961):—- any process that erases a bit must dump $k \log 2$ entropy into the environment. Landauer's principle applies universally to classical or quantum information (Bennett 1982).
- Erasure takes $|\psi\rangle \rightarrow |0\rangle$ for all $|\psi\rangle$. This cannot be performed by unitary transformation. Why? Suppose you could, then $|\psi\rangle \rightarrow |0\rangle$ and $|\phi\rangle \rightarrow |0\rangle$. Taking the inner product we have $\langle\psi|\phi\rangle = 1$ which is a contradiction.

- Our theorem applies to any process hiding a quantum state, whether by erasure, randomization, thermalization or any other procedure.

- Landauer's principle provides fundamental insight into thermodynamic reasonings. In contrast, data hiding provides more insight into the nature of thermalization processes. The terminology used above — input, output and ancilla — now takes on thermodynamic interpretations (e.g., initial system, final system, environment; or input system etc).

- In the case of a single system and environment, as the state of the system thermalizes, it contracts to a thermal distribution independent of its initial description.

- Perfect hiding implies complete thermalization, whereas imperfect hiding may shed some light on the approach to an equilibrium state.

- Either way, as the state vanishes from one subspace, it must appear in the remainder of Hilbert space.

Black Hole Information Loss

- How does this result apply to the black-hole information paradox?
- Hawking's work on black-hole evaporation precipitated a crisis in quantum physics. Whatever matter falls into it, a black hole evaporates in a steady stream of ideal featureless radiation.
- If we throw a pure state into a black hole we will get a mixed state: $|\Psi\rangle\langle\Psi| \longrightarrow \sigma$.
- Where has this information gone?

Options

There have been various proposals to resolve this paradox (Preskill hep-th/9209058).

- Information may come out during later stage.
- Information may be there in correlations between the quanta emitted early and the quanta emitted latter on.
- Information may be stored in a left out remnant.
- Information could be hidden in the correlation between the Hawking radiation and inside state of black hole.
- Collapse induces nucleation of a 'baby universe' and this new universe carries away the original information.

No-hiding theorem and Information loss

- In our formulation in-falling matter would correspond to subsystem I and out-going Hawking radiation would be subsystem O.

- The no-hiding theorem implies that no information is carried either within the out-going radiation or in correlations between the out-going radiation and anything else.

- Rejection of the correlations option is based on two assumptions: unitarity and Hawking's analysis.

- No-hiding theorem rigorously rules out any that the information escapes from the black hole but is nevertheless inaccessible as it is hidden in correlations between semi-classical Hawking radiation and the black hole's internal state.

- Provides a criterion to test any proposed resolution of the paradox. Any resolution that preserves unitarity must predict a breakdown in Hawking's analysis.

Summary

- Quantum information is fundamentally different than classical information.
- Copying, deleting, flipping, and partial erasure etc....are impossible in quantum world.
- No-hiding theorem provides new insight into the different laws governing classical and quantum information. Unlike classical information, QI cannot be completely hidden in correlations.
- Applications: Randomization, Quantum teleportation, Thermalization, Black hole evaporation and many more.
- *Whenever information disappears from one system it moves to somewhere else.*

Reference

[1] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Camb. Univ. Press, Cambridge, (2000).

[2] S. L. Braunstein and A. K. Pati, Edts. *Quantum Information with Continuous Variables*, Kluwer Academic Publisher, (2003).

[3] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

[4] D. Dieks, Phys. Lett. A **92**, 271 (1982).

[5] V. Buzek, M. Hillery and R. F. Werner, Phys. Rev. A **60**, R2626 (1999).

[6] A. K. Pati and S. L. Braunstein, Nature **404**, 164 (2000).

[7] R. Landauer, IBM J. Res. Dev. **3**, 183 (1961).

[8] C. H. Bennett, Int. J. Theor. Phys. **21**, 905 (1982).

[9] S. L. Braunstein and A. K. Pati, Phys. Rev. Lett. **98**, 080502 (2007).

THANK YOU