Quantum Communications

Concepts and Prospects

Apoorva Patel

Centre for High Energy Physics

Indian Institute of Science, Bangalore

18 July 2018, SPCOM 2018, IISc

Evolution of Communications

Life has explored a wide variety of communication systems over billions of years. The hallmark of evolution is the progressive increase in the range of communications:

- Molecular diffusion at the cellular level
- Electrochemical flows at the multi-cellular level
- Light and sound at the inter-organism level

Evolution of Communications

Life has explored a wide variety of communication systems over billions of years. The hallmark of evolution is the progressive increase in the range of communications:

- Molecular diffusion at the cellular level
- Electrochemical flows at the multi-cellular level
- Light and sound at the inter-organism level

The obvious shift from particles to waves offers well-known advantages. Preoccupation with looking at messages as ordered sequences of bits misses them.

Evolution of Communications

Life has explored a wide variety of communication systems over billions of years. The hallmark of evolution is the progressive increase in the range of communications:

- Molecular diffusion at the cellular level
- Electrochemical flows at the multi-cellular level
- Light and sound at the inter-organism level

The obvious shift from particles to waves offers well-known advantages. Preoccupation with looking at messages as ordered sequences of bits misses them.

Two ears and two eyes let us judge direction and distance of the communicator, by differential analysis of the two signals (a single signal does not have this information).

Evolution of Communications

Life has explored a wide variety of communication systems over billions of years. The hallmark of evolution is the progressive increase in the range of communications:

- Molecular diffusion at the cellular level
- Electrochemical flows at the multi-cellular level
- Light and sound at the inter-organism level

The obvious shift from particles to waves offers well-known advantages. Preoccupation with looking at messages as ordered sequences of bits misses them.

Two ears and two eyes let us judge direction and distance of the communicator, by differential analysis of the two signals (a single signal does not have this information).

- Knowing direction and distance helps in authentication.
- Interferometry allows astronomers to tremendously improve the signal-to-noise ratio (“superadditivity").

Wave correlations have important uses!

What is Quantum Communication?

It is a communication with quantum objects as message carriers (e.g. photons of the electromagnetic spectrum).

What is Quantum Communication?

It is a communication with quantum objects as message carriers (e.g. photons of the electromagnetic spectrum).

What must be exploited?

- Quantum objects have both particle and wave properties.
- They demonstrate that complex numbers are physical.
- Superposition allows multiple signals at the same point at the same time. All of them can be simultaneously processed, but only one of them can be selectively observed (e.g. radio or mobile phone transmissions).

What is Quantum Communication?

It is a communication with quantum objects as message carriers (e.g. photons of the electromagnetic spectrum).

What must be exploited?

- Quantum objects have both particle and wave properties.
- They demonstrate that complex numbers are physical.
- Superposition allows multiple signals at the same point at the same time. All of them can be simultaneously processed, but only one of them can be selectively observed (e.g. radio or mobile phone transmissions).

Present status

Laws of quantum mechanics are precisely known.
Elementary hardware components work as predicted.
Prototype quantum networks run around the clock.

DARPA network in Boston (2001): Raytheon BBN Technologies, Harvard University, Boston University, SECOCQ network in Vienna (2003), SwissQuantum network in Geneva (2010), Tokyo QKD network (2009), Beijing-Shanghai trunk line (2017).

Classical vs. Quantum

"Because the nature isn't classical, damn it . . ." —R.P. Feynman

Yet, input and output are always classical in problems relevent to us. So quantum dynamics can be exploited only at intermediate steps, with suitable encoding and decoding.

Classical vs. Quantum

"Because the nature isn't classical, damn it . . ." —R.P. Feynman

Yet, input and output are always classical in problems relevent to us. So quantum dynamics can be exploited only at intermediate steps, with suitable encoding and decoding.

Quantum fluctuations have been looked up on as "undesirable disturbances" in the classical setting.

We need to go to the other side, where classical noise becomes "unwanted nuisance" in the quantum setting.

Classical vs. Quantum

"Because the nature isn't classical, damn it . . ." —R.P. Feynman

Yet, input and output are always classical in problems relevent to us. So quantum dynamics can be exploited only at intermediate steps, with suitable encoding and decoding.

Quantum fluctuations have been looked up on as "undesirable disturbances" in the classical setting.

We need to go to the other side, where classical noise becomes "unwanted nuisance" in the quantum setting.

Information is quantified as entropy. Classical Shannon entropy is generalised to quantum von Neumann entropy.

$$H(\{p_i\}) = -\sum_i p_i \log p_i \longrightarrow S(\rho) = -\mathrm{Tr}(\rho \log \rho).$$

But a bit and a qubit are incomparable units of information. A single function cannot capture all quantum correlations.

New measures of correlations have to be constructed!

Quantum Correlations as Resource

Bell singlet state: $|\psi_{-}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$

Individual qubits behave randomly and carry no information.

But jointly the two qubits are perfectly (anti)correlated.

It can be considered a quantum version of one-time-pad, whose (anti)correlation is basis independent.

Quantum Correlations as Resource

Bell singlet state: $|\psi_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$

Individual qubits behave randomly and carry no information.
But jointly the two qubits are perfectly (anti)correlated.
It can be considered a quantum version of one-time-pad, whose (anti)correlation is basis independent.

Dense coding: A Bell state exists spread over two locations. One of the four operators $\{I, X, Z, XZ\}$ is applied to the half Bell state at one end, and the qubit is sent to the other end. Joint Bell basis measurement of the two qubits determines which of the four operators was applied.

$$|\psi_-\rangle \longrightarrow \{|\psi_-\rangle, -|\phi_-\rangle, |\psi_+\rangle, |\phi_+\rangle\}$$

Quantum Correlations as Resource

Bell singlet state: $|\psi_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$

Individual qubits behave randomly and carry no information.
But jointly the two qubits are perfectly (anti)correlated.
It can be considered a quantum version of one-time-pad, whose (anti)correlation is basis independent.

Dense coding: A Bell state exists spread over two locations. One of the four operators $\{I, X, Z, XZ\}$ is applied to the half Bell state at one end, and the qubit is sent to the other end. Joint Bell basis measurement of the two qubits determines which of the four operators was applied.

$$|\psi_-\rangle \longrightarrow \{|\psi_-\rangle, -|\phi_-\rangle, |\psi_+\rangle, |\phi_+\rangle\}$$

Teleportation: A Bell state exists spread over two locations. The unknown state to be teleported from one end is jointly measured with the half Bell state in the Bell basis. The two-bit measurement result sent to the other end recreates the unknown state from the other half of the Bell state.

$$|\alpha\rangle|\psi_-\rangle = \frac{1}{2}(-|\psi_-\rangle|\alpha\rangle + |\phi_-\rangle X|\alpha\rangle - |\psi_+\rangle Z|\alpha\rangle + |\phi_+\rangle XZ|\alpha\rangle)$$

Classical communication transfers quantum information!

What Produces Correlations?

- Common origin:

Initialises the signal states for multiple propagation paths.

Monochromaticity helps in keeping track of the phase information.

What Produces Correlations?

- Common origin:

Initialises the signal states for multiple propagation paths.

Monochromaticity helps in keeping track of the phase information.

- Conservation laws:

Products of multipartite or cascade decays have several constrained properties.

Energy, momentum, angular momentum, parity etc. are useful quantities.

What Produces Correlations?

- Common origin:

Initialises the signal states for multiple propagation paths.

Monochromaticity helps in keeping track of the phase information.

- Conservation laws:

Products of multipartite or cascade decays have several constrained properties.

Energy, momentum, angular momentum, parity etc. are useful quantities.

- Symmetries:

Identical bosons and fermions exist only in certain states.

Many systems relax to ground states with specific symmetries among components.

What Produces Correlations?

- Common origin:

Initialises the signal states for multiple propagation paths.

Monochromaticity helps in keeping track of the phase information.

- Conservation laws:

Products of multipartite or cascade decays have several constrained properties.

Energy, momentum, angular momentum, parity etc. are useful quantities.

- Symmetries:

Identical bosons and fermions exist only in certain states.

Many systems relax to ground states with specific symmetries among components.

Correlations are produced locally, but need to be used globally. For the intervening evolution to preserve them, interactions with the rest of the world must be suppressed.

Error correction is possible when signal and noise are on different separable scales.

Local error $\longrightarrow$ Add global redundancy.   Global error $\longrightarrow$ Find decoherence free subspace.

Communication Tasks

Shannon's theorems:

- Data compression is analogous to the classical case.

Schumacher: A message of n letters, where each letter is a pure quantum state independently drawn from the ensemble $\{|\psi_i\rangle, p_i\}$, can be asymptotically compressed to $nS(\rho)$ qubits, with $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. [Only bounds exist for ensembles of mixed states.]

Communication Tasks

Shannon's theorems:

- Data compression is analogous to the classical case.

Schumacher: A message of n letters, where each letter is a pure quantum state independently drawn from the ensemble $\{|\psi_i\rangle, p_i\}$, can be asymptotically compressed to $nS(\rho)$ qubits, with $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. [Only bounds exist for ensembles of mixed states.]

- Channel capacity is not analogous to the classical case.

Capacity depends on the type of information and the type of channel. Accessible classical information from quantum states is limited by projective measurements. It is $S(\rho)$ per letter for an ensemble of pure states, when the sender and the receiver can collectively address the entire message. It is less otherwise, upper bounded by the Holevo information when the message is a product state. [Tight bounds in other cases are not known.]

Communication Tasks

Shannon's theorems:

- Data compression is analogous to the classical case.

Schumacher: A message of n letters, where each letter is a pure quantum state independently drawn from the ensemble $\{|\psi_i\rangle, p_i\}$, can be asymptotically compressed to $nS(\rho)$ qubits, with $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. [Only bounds exist for ensembles of mixed states.]

- Channel capacity is not analogous to the classical case.

Capacity depends on the type of information and the type of channel. Accessible classical information from quantum states is limited by projective measurements. It is $S(\rho)$ per letter for an ensemble of pure states, when the sender and the receiver can collectively address the entire message. It is less otherwise, upper bounded by the Holevo information when the message is a product state. [Tight bounds in other cases are not known.]

Error correction: Each qubit has three error directions. Error correction is possible despite continuous variables, no cloning and irreversible measurements, because of discrete outcomes of projective measurements. Codes saturating the quantum Hamming bound exist.

Communication Tasks

Shannon's theorems:

- **Data compression is analogous to the classical case.**

Schumacher: A message of n letters, where each letter is a pure quantum state independently drawn from the ensemble $\{|\psi_i\rangle, p_i\}$, can be asymptotically compressed to $nS(\rho)$ qubits, with $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. [Only bounds exist for ensembles of mixed states.]

- **Channel capacity is not analogous to the classical case.**

Capacity depends on the type of information and the type of channel. Accessible classical information from quantum states is limited by projective measurements. It is $S(\rho)$ per letter for an ensemble of pure states, when the sender and the receiver can collectively address the entire message. It is less otherwise, upper bounded by the Holevo information when the message is a product state. [Tight bounds in other cases are not known.]

Error correction: Each qubit has three error directions. Error correction is possible despite continuous variables, no cloning and irreversible measurements, because of discrete outcomes of projective measurements. Codes saturating the quantum Hamming bound exist.

Entanglement concentration: n copies of non-maximally correlated ρ_{AB} can be converted to $nS(\rho_A)$ Bell state pairs, by measurement of global observables that project to the Schmidt decomposition basis.

Mixed states can be purified using branching produced by projective measurements.

Superadditivity of Quantum Resources

$\{|\psi\rangle \otimes |\psi\rangle, |\phi\rangle \otimes |\phi\rangle\}$ is more distinguishable than $\{|\psi\rangle, |\phi\rangle\}$.

This is a wave property. Astronomers use long exposure, and Fourier transform the received data, to pick out signals of specific frequency from the background noise.

Superadditivity of Quantum Resources

$\{|\psi\rangle \otimes |\psi\rangle, |\phi\rangle \otimes |\phi\rangle\}$ is more distinguishable than $\{|\psi\rangle, |\phi\rangle\}$.

This is a wave property. Astronomers use long exposure, and Fourier transform the received data, to pick out signals of specific frequency from the background noise.

$P(y_1, \ldots, y_n | x_1, \ldots, x_n) \neq \prod_{i=1}^{n} P(y_i | x_i)$, with suitably chosen codewords and collective decoding, even for independent inputs and a memoryless channel.

With only joint correlated detection, more information can be sent through an n-product channel than n times the amount that can be sent through a single use of the channel. Quantum correlations between the codewords provide the extra channel capacity.

Superadditivity of Quantum Resources

$\{|\psi\rangle \otimes |\psi\rangle, |\phi\rangle \otimes |\phi\rangle\}$ is more distinguishable than $\{|\psi\rangle, |\phi\rangle\}$.

This is a wave property. Astronomers use long exposure, and Fourier transform the received data, to pick out signals of specific frequency from the background noise.

$P(y_1,\ldots,y_n|x_1,\ldots,x_n) \neq \prod_{i=1}^n P(y_i|x_i)$, with suitably chosen codewords and collective decoding, even for independent inputs and a memoryless channel.

With only joint correlated detection, more information can be sent through an n-product channel than n times the amount that can be sent through a single use of the channel. Quantum correlations between the codewords provide the extra channel capacity.

The transmission rate strictly increases with the number of jointly detected outputs n. For classical information sent over a quantum channel, the Holevo capacity is the $n \to \infty$ limit: $C^{(1)}(\mathcal{E}) = \max\limits_{\{p_x,\rho_x\}} [S(\rho) - \sum_x p_x S(\rho_x)]$.

For quantum information sent over quantum channel, the capacity is less well understood.

Superadditivity of Quantum Resources

$\{|\psi\rangle \otimes |\psi\rangle, |\phi\rangle \otimes |\phi\rangle\}$ is more distinguishable than $\{|\psi\rangle, |\phi\rangle\}$.

This is a wave property. Astronomers use long exposure, and Fourier transform the received data, to pick out signals of specific frequency from the background noise.

$P(y_1, \ldots, y_n | x_1, \ldots, x_n) \neq \prod_{i=1}^{n} P(y_i|x_i)$, with suitably chosen codewords and collective decoding, even for independent inputs and a memoryless channel.

With only joint correlated detection, more information can be sent through an n-product channel than n times the amount that can be sent through a single use of the channel. Quantum correlations between the codewords provide the extra channel capacity.

The transmission rate strictly increases with the number of jointly detected outputs n. For classical information sent over a quantum channel, the Holevo capacity is the $n \to \infty$ limit: $C^{(1)}(\mathcal{E}) = \max_{\{p_x, \rho_x\}} [S(\rho) - \sum_x p_x S(\rho_x)]$.

For quantum information sent over quantum channel, the capacity is less well understood.

- Zero capacity channels can be combined to obtain a nonzero communication rate.
- Perfect entanglement between inputs to the channels can even eliminate the noise.
- The same logic applies to other iterative processes, e.g. quantum thermal engines.

Quantum Random Number Generation

Random numbers are used for critical security and reliability checks. Applications range from cryptosystems to gaming.

Hardware random number generators use unpredictable physical processes, and can be tested by data compression algorithms. Classical ones hide determinism behind noise complexity (e.g. chaotic systems), and are vulnerable to environmental perturbations.

Quantum Random Number Generation

Random numbers are used for critical security and reliability checks. Applications range from cryptosystems to gaming.

Hardware random number generators use unpredictable physical processes, and can be tested by data compression algorithms. Classical ones hide determinism behind noise complexity (e.g. chaotic systems), and are vulnerable to environmental perturbations.

Quantum randomness is intrinsic. Quantum optics provides simple, compact and low-cost random number generators.

Bias in the physical processes is easily removed by the von Neumann-Peres scheme.

Quantum random number generators based on radioactive decays are bulky and slow.

Quantum Random Number Generation

Random numbers are used for critical security and reliability checks. Applications range from cryptosystems to gaming.

Hardware random number generators use unpredictable physical processes, and can be tested by data compression algorithms. Classical ones hide determinism behind noise complexity (e.g. chaotic systems), and are vulnerable to environmental perturbations.

Quantum randomness is intrinsic. Quantum optics provides simple, compact and low-cost random number generators.

Bias in the physical processes is easily removed by the von Neumann-Peres scheme.

Quantum random number generators based on radioactive decays are bulky and slow.

Quantis from ID Quantique (since 2001):

Single photons from a light emitting diode are split into two paths and recorded with two detectors. After acquisition and status checks, followed by unbiasing, certified random bit sequence is produced at Mbps rates. [Available as a USB device or a PCI Express card.]

Shot noise Poisson process detection of photons in mobile phone cameras can be used as a random number generator. [Phys. Rev. X 4 (2014) 031056]

Quantum Communication Hardware

Essential devices are sources, repeaters and detectors, all operating at the single photon level.

The transmission wavelength bands are dictated by the properties of the telecommunications fibre, and the transparency of the atmosphere.

Quantum Communication Hardware

Essential devices are sources, repeaters and detectors, all operating at the single photon level.

The transmission wavelength bands are dictated by the properties of the telecommunications fibre, and the transparency of the atmosphere.

Sources:

Photons cannot be produced on demand. Heralded production is needed for fixing the time window.

The signal is better encoded in the phase than in polarization.

Possibilities are: Frequency combs in waveguides, Er^{3+} ions in YSO, ...

Quantum Communication Hardware

Essential devices are sources, repeaters and detectors, all operating at the single photon level.

The transmission wavelength bands are dictated by the properties of the telecommunications fibre, and the transparency of the atmosphere.

Sources:

Photons cannot be produced on demand. Heralded production is needed for fixing the time window.

The signal is better encoded in the phase than in polarization.

Possibilities are: Frequency combs in waveguides, Er^{3+} ions in YSO, . . .

Repeaters (trusted nodes):

Required for long distance (> 80km for fibre) transmission.

The signal is first stored in quantum memory and then retransmitted after error correction.

Amplifiers cannot be used. Redundancy is used to bypass the no-cloning constraint.

Quantum Communication Hardware

Essential devices are sources, repeaters and detectors, all operating at the single photon level.

The transmission wavelength bands are dictated by the properties of the telecommunications fibre, and the transparency of the atmosphere.

Sources:

Photons cannot be produced on demand. Heralded production is needed for fixing the time window.

The signal is better encoded in the phase than in polarization.

Possibilities are: Frequency combs in waveguides, Er^{3+} ions in YSO, ...

Repeaters (trusted nodes):

Required for long distance (> 80km for fibre) transmission.

The signal is first stored in quantum memory and then retransmitted after error correction.

Amplifiers cannot be used. Redundancy is used to bypass the no-cloning constraint.

Detectors:

Fast sensitive response and short dead time needed.

Suitable materials have to be found. Hybrid layered 2D systems are a possibility.

Important Features

Quantum key distribution protocols detect eavesdroppers.

Distillable frame-independent correlations allow device independent protocols, for perturbations below a threshold.

Self-testing strategies can be implemented on trusted nodes.

Important Features

Quantum key distribution protocols detect eavesdroppers.

Distillable frame-independent correlations allow device independent protocols, for perturbations below a threshold.

Self-testing strategies can be implemented on trusted nodes.

In Pipeline

- Fibre-based trusted-node backbone quantum networks.
- Free space quantum communication using satellites.
- Development of low-cost hand-held access devices.

Important Features

Quantum key distribution protocols detect eavesdroppers.

Distillable frame-independent correlations allow device independent protocols, for perturbations below a threshold.

Self-testing strategies can be implemented on trusted nodes.

In Pipeline

- Fibre-based trusted-node backbone quantum networks.
- Free space quantum communication using satellites.
- Development of low-cost hand-held access devices.
- Improvement in performance of quantum components: sources, interfaces, memories and detectors.
- Quantum key distribution rates >100 Mbps.
- Integrated systems with multiplexing of signals.

Important Features

Quantum key distribution protocols detect eavesdroppers.

Distillable frame-independent correlations allow device independent protocols, for perturbations below a threshold.

Self-testing strategies can be implemented on trusted nodes.

In Pipeline

- Fibre-based trusted-node backbone quantum networks.
- Free space quantum communication using satellites.
- Development of low-cost hand-held access devices.
- Improvement in performance of quantum components: sources, interfaces, memories and detectors.
- Quantum key distribution rates >100 Mbps.
- Integrated systems with multiplexing of signals.
- Cryptographic algorithms and secret-sharing protocols.
- MIMO communication systems with enhanced signal-to-noise ratio using interferometry.

Post-quantum Cryptography

Quantum algorithms can break cryptographic codes based on abelian fields (e.g. RSA and discrete logarithms).

But they are unable to break cryptographic codes based on non-abelian fields (e.g. elliptic curve isogenies, lattices).

Post-quantum Cryptography

Quantum algorithms can break cryptographic codes based on abelian fields (e.g. RSA and discrete logarithms).

But they are unable to break cryptographic codes based on non-abelian fields (e.g. elliptic curve isogenies, lattices).

Post-quantum cryptography uses classical communication protocols that are secure against quantum attackers.

It requires rigorous cryptanalysis (security proofs) for quantum-safe key agreements and signatures.
Authentication problem remains.

Post-quantum Cryptography

Quantum algorithms can break cryptographic codes based on abelian fields (e.g. RSA and discrete logarithms).

But they are unable to break cryptographic codes based on non-abelian fields (e.g. elliptic curve isogenies, lattices).

Post-quantum cryptography uses classical communication protocols that are secure against quantum attackers.

It requires rigorous cryptanalysis (security proofs) for quantum-safe key agreements and signatures.
Authentication problem remains.

Why is this attractive?

Quantum signals have the lowest possible intensity, and so are the easiest to jam.

Quantum communication rates are suppressed by the need to relax the detector to a quiet state after every observation.

Quantum Technologies

The field of quantum technologies is poised for significant breakthroughs in the coming years. Many organizations have formulated detailed roadmaps.

Europe roadmap: https://arXiv.org/abs/1712.03733

USA roadmap: https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Quantum_Info_Sci_Report_2016_07_22%20final.pdf

Quantum Technologies

The field of quantum technologies is poised for significant breakthroughs in the coming years. Many organizations have formulated detailed roadmaps.

Europe roadmap: https://arXiv.org/abs/1712.03733

USA roadmap: https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Quantum_Info_Sci_Report_2016_07_22%20final.pdf

The essential features that contribute to these technologies are superposition, entanglement, squeezing and tunneling of quantum states.

Quantum Technologies

The field of quantum technologies is poised for significant breakthroughs in the coming years. Many organizations have formulated detailed roadmaps.

Europe roadmap: https://arXiv.org/abs/1712.03733

USA roadmap: https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Quantum_Info_Sci_Report_2016_07_22%20final.pdf

The essential features that contribute to these technologies are superposition, entanglement, squeezing and tunneling of quantum states.

Practical applications are expected to appear

- first in sensing and metrology,
- then in communications and simulations,
- then as feedback to foundations of quantum theory,
- and ultimately in computation.

Quantum Technologies

The field of quantum technologies is poised for significant breakthroughs in the coming years. Many organizations have formulated detailed roadmaps.

Europe roadmap: https://arXiv.org/abs/1712.03733
USA roadmap: https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Quantum_Info_Sci_Report_2016_07_22%20final.pdf

The essential features that contribute to these technologies are superposition, entanglement, squeezing and tunneling of quantum states.

Practical applications are expected to appear

- first in sensing and metrology,
- then in communications and simulations,
- then as feedback to foundations of quantum theory,
- and ultimately in computation.

Developments in quantum technologies will also push classical technologies in new directions.