Power of Entanglement in Quantum Communication

Seth Lloyd
d'Arbeloff Laboratory for Information Systems and Technology, Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139
(Received 28 May 2002; published 22 April 2003)

A communication channel is a physical system that transfers information from one place to another. Examples of communication channels include wires, optical fibers, and chains of spins that propagate spin waves through a medium. This Letter shows that the power-limited communication capacity of a multimode optical fiber or a set of parallel spin chains can be enhanced by introducing nonlinear couplings between the modes or chains. In particular, M coupled, entangled modes can send M bits in the same time it takes a single mode to send a single bit, and in the same time it takes M uncoupled, unentangled modes to send $\sqrt{M}$ bits.

DOI: 10.1103/PhysRevLett.90.167902 PACS numbers: 03.67.Hk, 42.79.Sz, 84.40.Ua

As communication technologies push down to the quantum level, a considerable effort has been made to uncover the physical limits to the communication process, with special emphasis on the bosonic communications channel [1]. Quantum systems can be correlated with each other in ways that classical systems cannot, a feature known as entanglement. This Letter investigates how the capacity of communication channels can be enhanced by coupling together information-propagating degrees of freedom via a nonlinear dynamics to induce an entangled state in the process of transmission. In contrast, previous results have investigated enhancements to the communication capacity of uncoupled quantum channels by exploiting preexisting entanglement [2–6]. Here it is shown that for fixed power, M coupled, entangled spin chains or modes of the electromagnetic field can in principle transmit information at a rate $\sqrt{M}$ times greater than M uncoupled, unentangled chains, or modes.

All physical channels are at bottom quantum mechanical, and quantum mechanics restricts the rate at which information can be transmitted down noiseless channels at finite power. (Since the capacity of a classical channel scales logarithmically with its signal to noise ratio, the capacity of a classical noiseless channel such as a field mode in a fiber is typically infinite even in the limit that power goes to zero.) In particular, it is well established via the use of Kholevo's theorem [1,7] that a noiseless broadband bosonic channel such as a single transverse mode of the electromagnetic field with power P can transmit $C_1 = \alpha\sqrt{P/\hbar}$ bits per second, where $\alpha = \sqrt{\pi/3}(1/\ln 2)$. The power P is equal to the energy E used to transmit the information, divided by the total time t over which the transmission takes place: as noted in [8], this energy need not be dissipated in the course of transmission. As a consequence, if the power is spread among M unentangled broadband bosonic channels, each with power P/M, the rate of communication is $C_M^C = \sqrt{M}C_1$. This is the best rate known for power-limited communication using M unentangled channels [1]. For noiseless channels, Refs. [4,5] imply that this rate cannot be surpassed merely by entangling the states of the channels while leaving their dynamics unchanged.

By contrast, it will be shown here that if one couples together M spin chains or tranverse modes of the electromagnetic field to induce entanglement between the modes in the course of propagation, then using power P one can send information from A to B at a rate $C_M^Q = \beta M\sqrt{P/\hbar} \approx MC_1 = \sqrt{M}C_M^C$, where $\beta = \sqrt{2/\pi(1-2^{-M})}$. That is, for a fixed power, entangled chains or modes can in principle outperform unentangled chains or modes by a wide margin for large M. Perhaps more remarkably, M entangled modes can send M bits in the same time and using the same overall power that it takes a single mode to send a single bit. Not surprisingly, producing the necessary entangling dynamics for M spin chains or modes is likely to prove difficult. As will be shown, however, simple demonstrations of the power of a small number of entangled channels can be performed using existing techniques of quantum information processing.

To determine the effect of an entangling dynamics on information propagation, a simpler channel model is analyzed—the "qubit" channel. The qubit channel immediately generalizes to channels consisting of spin chains and to modes of the electromagnetic field.

The qubit channel transmits a quantum bit from A to B. Suppose that A and B each possess a two-state quantum system, or qubit. A's qubit holds the quantum state $|\psi\rangle$ which is to be transmitted to B, whose qubit is initially in the state $|0\rangle$. The two states $|0\rangle$ and $|1\rangle$ of the qubits are assumed to be degenerate, so that no energy is required to store the qubit. The qubit channel can be used either to transmit classical information—$|\psi\rangle = |0\rangle$ or $|1\rangle$—or to transmit quantum information—$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$. The dynamics of the channel should transfer the information from A's qubit to B's qubit. After the transfer has taken place, B's qubit is in the state $|\psi\rangle$ and A's qubit is in a standard state such as $|0\rangle$.

The laws of quantum mechanics [9] then bound the rate of information transmission down the qubit channel given limited power. The average overlap $|\langle 0|\psi\rangle|^2$ of A and B's initial state with their final state is $1/2$. Accordingly, each time the channel is used, the total state of A and B together with the channel must evolve by an average angle in Hilbert space of at least $\pi/2$. That is, to transmit a 0 requires no transformation of B's qubit, but to transmit a 1, B's qubit must be rotated by π. When a 0 is sent, no transformation of B's qubit takes place and no energy is required: $E_0 = 0$. But when a 1 is sent, the Margolus-Levitin theorem [10] implies that when B's qubit is rotated by π, the average energy of the complete system above its ground state must be at least $E_1 \geq \pi\hbar/2\Delta t$, where Δt is the time over which the transfer takes place (see also [11,12]). If a 1 is sent with probability p_1, the power is $P = \langle E\rangle/\Delta t \geq \pi\hbar/4\Delta t^2$, where $\langle E\rangle = p_0E_0 + p_1E_1$. If a 1 is sent half the time, then a bit is transferred from A to B at a rate

$$C_1^Q = 1/\Delta t = (2/\sqrt{\pi})\sqrt{P/\hbar}. \tag{1}$$

The power-limited transmission rate of the qubit channel differs from that of the broadband bosonic channel capacity by a constant of order unity.

The above argument shows why power is the limiting quantity for information transmission. Energy limits the speed with which any quantum-mechanical transformation takes place: to make something happen, e.g., a bit go from here to there, in time Δt requires energy $\sim\hbar/\Delta t$ to be invested in whatever system is performing the transformation. Since energy $\sim\hbar/\Delta t$ is being invested for time Δt, the power $P = E/\Delta t$ goes as $\sim\hbar/\Delta t^2$. Accordingly, the rate at which any transformation can take place given power P is $1/\Delta t \sim \sqrt{P/\hbar}$. The rate of transformation is limited by the square root of the available power, whether that transformation is communication, computation, or work. The results derived here for limits to quantum communication channels are closely related to the fundamental limits to computation derived in [12]. Indeed, the maximum rate at which quantum logic operations can be performed is also given by $1/\Delta t \sim \sqrt{P/\hbar}$, where P is the power invested in performing the operation.

The energy invested in communication need not be dissipated [8]. In the bosonic channel, the energy is typically transmitted down the channel. In the case of channels such as the spin chains discussed below, the energy invested in communication goes into interactions between the spins along the chain, allowing information-bearing excitations to propagate along the chain.

A particularly simple communication channel is that between adjacent bits in a quantum computer [13]. Consider, for example, a simple NMR quantum information processor consisting of a carbon 13 doped alanine molecule. The backbone of the molecule consists of a chain of three covalently bonded carbon 13 atoms. In room-temperature NMR, the spins of the carbon 13 nuclei interact via the electrons in the bonds. These interactions can be used to propagate information from atom to atom at a rate $1/\Delta t$ close to $\sqrt{E/\hbar\Delta t}$, where E is the interaction energy between adjacent spins. (It is the interaction energy that governs the transfer rate: the energies in the microwaves and in the magnets in NMR are, of course, much greater.) That is, existing quantum logic devices can swap information from one place to another at rates that are governed by Eq. (1), with minimal dissipation during the transfer process.

Equation (1) applies to the reliable transmission of a single bit. If one is willing to send less than a full bit of information by sending a 0 with a higher probability, one can decrease the energy per transmission time Δt. This "poor student" strategy can increase the power-limited transmission rate by a fraction $h(q)/\sqrt{2q}$, where q is the probability of sending a 1, and $h(q) = -q\log_2 q - (1-q)\log_2(1-q)$. The maximum increase obtainable by the poor student strategy is a factor of 1.1475 for $q = 0.2415$. In addition, if one is willing to use error correcting codes, then the average transfer time can be less than $\Delta t = \pi\hbar/4E$, as one does not have to rotate the state of A and B by the full angle π: one can enhance the transmission rate by rotating by slightly less than π and having B measure his qubit. The maximum enhancement in power-limited communication rates that can be obtained by such techniques is not known.

A simple example of an interaction that attains the qubit communication rate (1) is the application of a "swap" operation: $S = \sum_{ij=0}^{1} |ij\rangle_{AB}\langle ji|$. S is a unitary transformation that swaps the quantum information in A's qubit with the quantum information in B's qubit: $S|\psi\rangle_A \otimes |\phi\rangle_B = |\phi\rangle_A \otimes |\psi\rangle_B$, for all states $|\phi\rangle, |\psi\rangle$. Note that $S^2 = 1$: two applications of S return the bits to their original states. Consequently, S is Hermitian and has eigenvalues ± 1. Note also that $e^{-i\theta S} = \cos\theta - i\sin\theta S$.

Swap is a natural Hamiltonian for a variety of physical processes, including the exchange interaction between electrons. Two electrons interacting via a Heisenberg-like interaction with average energy E above the ground state energy will in fact swap the information registered by their spins in a time $\Delta t = \pi\hbar/2E$, thereby saturating the limit of Eq. (1). If one waits for a second time step Δt, the interacting electrons will swap the information back again.

Now analyze the power applied during a swap operation. The power is the average energy of the swap interaction divided by the time over which the interaction takes place. Apply the Hamiltonian $\tilde{S} = \pi\hbar(1-S)/2\Delta t$ to A and B's qubits for time Δt swaps the qubits: $e^{-i\tilde{S}\Delta t/\hbar} = S$. The average energy of A and B during the swap is

$$E = (\langle\psi|_A\langle 0|_B)\tilde{S}(|\psi\rangle_A|0\rangle_B) = \pi\hbar(1 - |\langle 0|\psi\rangle|^2)/2\Delta t. \tag{2}$$

Averaging over states $|\psi\rangle$ gives an energy E that saturates the Margolus-Levitin bound. Swap attains the power/capacity limit of Eq. (1) above. It does so coherently and without dissipation in principle. As noted above, a variety of microscopic physical systems including existing quantum logic devices can swap information from one place to another at rates very close to this limit.

The swap picture of quantum information transmission assumes a direct transfer of A's qubit to B. A similar picture holds in which A's and B's qubits are coupled by an intervening chain of qubits $A_1B_1A_2B_2 \ldots A_nB_n$, where A has access to A_1 and B has access to B_n. Here, quantum information can be sent along the chain by swapping A_i with B_i over a time $\Delta t/2$, then swapping B_i with A_{i+1}, and repeating until the qubit has been moved from A to B. In this case, the time taken to send a qubit from A to B is $n\Delta t$, and the average energy employed is $2nE$, giving an average power of $P = 2E\Delta t$. The rate at which information is sent down the channel is still 1 bit in time Δt. Accordingly, the transmission of information from A to B by repeated swapping down a chain of qubits comes within $\sqrt{2}$ of the the power/capacity limit of (1). Note that repeated swaps move qubits from A to B and from B to A simultaneously, so that the net transmission of energy down the channel is zero even though the power is nonzero. A variety of Hamiltonians (e.g., $H = S_{A_1B_1} + S_{B_1A_2} + \ldots S_{A_nB_n}$) can be used to propagate spin waves down the qubit chain at rates on the order of the power/capacity limit (1).

The similarity of the power/capacity tradeoff for chains of qubits and for particles such as bosons should not be surprising as the physics of spin wave propagation is closely related to the physics of particle propagation. In fact, a chain of spins interacting according to a ferromagnetic Heisenberg interaction is well known to be equivalent to a system of propagating fermions [14], which are also known [1] to support a maximum transmission rate that goes as $\sqrt{P/\hbar}$.

Now investigate the case of multiple qubit channels that can be coupled to each other during the course of propagation. It is here that entanglement leads to a significant enhancement in power-limited transmission rate. Clearly, M uncoupled qubit channels can transmit information at a rate $\sqrt{M}$ greater than a single quantum channel using the same power P merely by dividing the power equally among the channels. Each channel now transmits at a rate $(2/\sqrt{\pi})\sqrt{P/M\hbar}$ giving an overall rate of transmission $\tilde{C}_M^C = (2M/\sqrt{\pi})\sqrt{P/Mh} = (2/\sqrt{\pi})\sqrt{MP/h} = \sqrt{M}\tilde{C}_1$ (here the tilde ˜ indicates that the capacity is that of the qubit channel rather than the bosonic channel). This rate enhancement is the best enhancement known for parallel unentangled channels and holds for both the bosonic channel and for the qubit channel.

If one is able to engineer interactions that entangle the qubit channels in the process of transmission, one can do even better, as will now be shown. The goal of the M-channel transfer is to enact the $2M$-qubit analog of the swap above: $S_{1\ldots M} = S_1S_2 \ldots S_M$, where S_1 is the swap operator on the first of A and B's qubit channels, S_2 is the swap operator on the second, etc., The $2M$-qubit swap $S_{1\ldots M}$ swaps A's M qubits with B's M qubits and has the same properties as the 2-qubit swap above (Hermitian, squares to one, etc.). As above, define the Hamiltonian $\tilde{S}_{1\ldots M} = \pi\hbar(1 - S_{1\ldots M})/2\Delta t$. Applying the Hamiltonian $\tilde{S}_{1\ldots M}$ for a time Δt then swaps A's qubit string with B's qubits. The average energy during the M-qubit swap is $E = \pi\hbar(1 - |\langle 0|\psi\rangle|^2)/2\Delta t$, as in Eq. (2) above. Now, however, $|\langle 0|\psi\rangle|^2 = 1/2^M$ for a randomly selected $|\psi\rangle$. Accordingly, the time taken to transfer A's bit to B using power P is given by $1/\Delta t = \sqrt{2(1 - 2^{-M})P/\pi\hbar}$, which is the M-channel analog of the limit (1). The time taken to perform the transfer using power P comes within $\sqrt{2}$ of the limit (1), but now for the transfer of M bits rather than a single bit.

It is easy to verify that during the transfer, the M qubit channels are mutually entangled. For example, if A's input state is $|b_M\rangle = |b_1 \ldots b_M\rangle$, then at time $\Delta t/2$ (halfway through the controlled flipping operation) A and B's qubits are in the state

$$\frac{e^{-i\pi/4}}{\sqrt{2}}(|b_1 \ldots b_M\rangle_A|00\ldots 0\rangle_B + i|00\ldots 0\rangle_A|b_1 \ldots b_M\rangle_B). \tag{3}$$

Note that decohering the state of the channel part way through the transmission still leaves B with a significant amount of information. That is, as in the single qubit case, if B measures his qubits before the full transmission time Δt, he still obtains the correct message with a nonzero probability.

Application of the Hamiltonian $\tilde{S}_{1\ldots M}$ transfers M bits down M parallel qubit channels using essentially the same energy $E \approx \hbar/\Delta t$, the same power $P \approx \hbar/\Delta t^2$, and in the same time Δt it takes a single channel to transmit a single bit. Similar results hold for the transmission of M qubits down M chains of n qubits, as above: the transmission time in this case is n times as long, but the power is the same as the single qubit case, while the number of bits per second is M times the single qubit channel rate.

Transferring M bits down M uncoupled, unentangled quantum channels corresponds to the application of M two-qubit swap operations with Hamiltonian $\tilde{S}_1 + \ldots + \tilde{S}_M$, as opposed to the $2M$-qubit swap Hamiltonian $\tilde{S}_{1\ldots M} = \tilde{S}_1\tilde{S}_2 \ldots \tilde{S}_M$, and takes $\sqrt{M}$ times the energy of the entangled swap. As a result, the coupled, entangled channels have a capacity of at least $\sqrt{M}$ times the capacity of the uncoupled, unentangled channels. To find the absolute upper bound on the capacity of coupled quantum channels will require the detailed application of Kholevo's theorem [1,7].

In a certain sense, that it is just as easy in terms of power and energy to rotate $2M$ bits from one state to another as it is to rotate 2 bits from one state to another should not be surprising: no two states in Hilbert space are more than angle of π apart. Accordingly, if one can effect arbitrary evolutions on the M-qubit channel Hilbert space, M bits can be transferred using the same power and time as 1 bit. Effectively, the coupling between the channels allows them to transmit information in the form a "superparticle" with 2^M internal states. The $\sqrt{M}$ enhancement afforded by exploiting entanglement is typical of quantum information processing and arises from essentially the same source as the $\sqrt{M}$ enhancements in quantum search [15] and quantum positioning [16].

The catch is that enacting the necessary Hamiltonian $\tilde{S}_{1\ldots M}$ is likely to prove experimentally difficult. Even for two-qubit channels, enacting the Hamiltonian of Eq. (2) involves entangling four quantum bits, a difficult action using current technologies. One might hope to be able to build up this Hamiltonian time evolution using elementary quantum logic operations on two quantum bits at a time, but in this case most of the power advantage is lost, as the net angle rotated in Hilbert space becomes larger than π. To attain the $\sqrt{M}$ enhancement of channel capacity allowed by entanglement, an M-qubit entangling operation must be used. The single qubit channel swap operator between A and B corresponds to a Hamiltonian $\sigma_x^A\sigma_x^B + \sigma_y^A\sigma_y^B + \sigma_z^A\sigma_z^B$, and the corresponding operator for swapping particles such as photons between A and B is $a_A a_B^\dagger + a_A^\dagger a_B$. The M-channel swap operator $S_{1\ldots M}$ is the product $S_1 S_2 \ldots S_M$ of the individual swap operators: such operations correspond to interaction operators of the form $\sigma_x^1\sigma_x^2\ldots\sigma_x^M$ for spin qubits and $a_{A1}a_{B1}^\dagger \ldots a_{AM}a_{BM}^\dagger$ + H.c. for particle modes. That is, Mth order nonlinear interactions are required to attain the entanglement-enhanced channel capacity presented here. Such interactions are hard to enact experimentally, although it is possible to use simple quantum logic and quantum communication devices to perform proof-of-principle demonstrations of entanglement-enhanced capacity for small M. For example, suppose that A wants to use microwaves or light to load 2 bits onto the nuclear spins or hyperfine levels of B's two atoms. The results derived above show that if A is able to manipulate entangling interactions between the two spins or atoms, the 2 bits can be loaded using $\sqrt{2}$ less power than in the case that the spins or atoms remain unentangled. Such a proof-of-principle experiments based on existing techniques for performing quantum logic [13] could be performed using nuclear resonance on two spins in a molecule, or using optical resonance on two interacting atoms or ions in a trap.

For larger M, enacting the proper entangling coupling is likely to prove experimentally difficult, but if such coupling can be enacted, substantial gains in quantum channel capacity can be obtained. Whether or not the potential gains afforded by entanglement can be realized in experimentally feasible quantum optical systems acting over significant distances remains an open question. Additional open questions include the effect of noise on entangling channels, and whether partial entanglement allows a lesser but still significant communication enhancement. But as this Letter shows, entanglement in principle gives a significant increase in channel capacity.

This work was supported by ARDA/NRO, CMI, DARPA, and NSF. The author would like to thank Vittorio Giovannetti, Lorenzo Maccone, Aram Harrow, Hermann Haus, Jeff Shapiro, and Franco Wong for inspiration and for helpful discussions.

[1] C. M. Caves and P. D. Drummond, Rev. Mod. Phys. **66**, 481–537 (1994), and references therein.
[2] E. H. Lieb and M. B. Ruskai, J. Math. Phys. (N.Y.) **14**, 1938 (1973).
[3] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[4] B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).
[5] A. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998).
[6] C. H. Bennett, P.W. Shor, J. A. Smolin, and A.V. Thapliy, quant-ph/0106052.
[7] A. S. Kholevo, Probl. Pereda. Inf. **9**, 3 (1973) [Probl. Inf. Transm. **9**, 177 (1973)].
[8] R. Landauer, Nature (London) **335**, 779 (1988).
[9] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Hingham, 1995), Chap. 5.
[10] N. Margolus and L. B. Levitin, in *PhysComp96*, edited by T. Toffoli, M. Biafore, and J. Leao (NECSI, Boston, 1996); Physica (Amsterdam) **120D**, 188 (1998).
[11] G. N. Fleming, Nuovo Cimento Soc. Ital. Phys. **16A**, 232 (1973).
[12] S. Lloyd, Nature (London) **406**, 1047 (2000).
[13] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[14] V. E. Korepin, *Quantum Inverse Scattering Method and Correlation Functions, Cambridge Monographs on Mathematical Physics* (Cambridge University Press, Cambridge, 1993).
[15] L. K. Grover, in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing* (ACM Press, New York, 1996), pp. 212–218.
[16] V. Giovannetti, S. Lloyd, and L. Maccone, Nature (London) **412**, 417 (2001).