ENTANGLEMENT AND CHANNEL CAPACITY

SETH LLOYD
Massachusetts Institute of Technology, Department of Mechanical Engineering,
Cambridge, MA 02139, USA

This paper investigates the capacity of quantum channels, and shows that enhancements in channel capacity can be obtained by coupling together the information degrees of freedom in quantum channels. By coupling together modes in a multimode optical fiber, one can in principle obtain a significant enhancement of the capacity of the fiber for fixed power over the same fiber with uncoupled modes.

Communication channels, like all physical systems, are at bottom quantum mechanical, and their physical limits are calculated using the laws of quantum mechanics.[1−22] A variety of results suggest that enhancements in channel capacity can be obtained by exploiting techniques of quantum information processing.[23−26] For example, quantum systems can be correlated with each other in ways that classical systems cannot, a feature known as entanglement. It has been speculated that entanglement might be used enhance the capacity of quantum communication channels.[24−28] In general, the amount by which entanglement can enhance communication is not known.

A recent paper by the author[29] investigates the question of whether it is possible to enhance the capacity of communication channels by coupling together their information-bearing degrees of freedom in a way that induces entanglement. That paper showed that for fixed power, M coupled, entangled spin chains or modes of the electromagnetic field can in principle transmit information at a rate at least $\sqrt{M}$ times greater than M uncoupled, unentangled chains or modes. Presented herein is a summary of those results.

To understand how quantum mechanics allows enhancements of communication capacity, first review the case of unentangled parallel quantum channels. In particular, it is well established[1−22] that the broadband bosonic channel (a single transverse mode of the electromagnetic field) with power P can transmit $C_{1q} = \alpha\sqrt{P/\hbar}$ bits per second, where $\alpha = \sqrt{\pi/3}(1/\ln 2)$. A similar result holds for propagation of information down spin chains. (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 Refs. 8,17, this energy need not be dissipated in the course of transmission.) As a consequence,[1] if the power is spread amongst M unentangled broadband bosonic channels, each with power P/M, the rate of communication is $C_{Mc} = \sqrt{M}C_{1q}$. This is the best known rate for power-limited communication using M unentangled channels, though it is not proven to be the limiting rate. For noiseless channels, however, Refs. 26,27 imply that this rate cannot be surpassed merely by entangling the states of the channels while leaving their dynamics unchanged. By contrast, in Ref. 29 the author showed that if one couples together M spin chains or transverse 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 $C_{Mq} = \sqrt{2/\pi(1-2^{-M})}M\sqrt{P/\hbar} \approx MC_1 = \sqrt{M}C_{Mc}$. That is, for a fixed power, dynamics that entangle chains or modes can in principle outperform by a factor of $\sqrt{M}$ dynamics that leave the chains or modes unentangled.

To analyze the effect of an entangling dynamics on information propagation, consider a qubit channel that transmits a quantum bit from A to B. Initially, 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 — $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. The dynamics of the channel transfers 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 sole restriction placed on dynamics of the channel is that it obeys the rules of quantum mechanics: the time evolution of A's qubit and B's qubit, together with their environment and whatever interaction they use to transfer the information, is a unitary, Hamiltonian dynamics. (An arbitrary strictly positive time evolution can be embedded in such dynamics.[30]) This requirement bounds the rate of reliable information transmission down the qubit channel for any possible dynamics given limited power.

Quantum dynamics obey the Margolus-Levitin theorem, which implies that when B's qubit is rotated by π, the average energy of the complete system above its ground state is $E \geq \pi\hbar/2\Delta t$, where Δt is the time over which the transfer takes place.[31] In Ref. 29, the Margolus-Levitin theorem was used to show that the maximum rate at which information can be sent down the qubit channel is $C_{1q} = 1/\Delta t = (2/\sqrt{\pi})\sqrt{P/\hbar}$. This result holds for any dynamics that reliably transfers the qubit from A to B. In other words, the power-limited capacity of the qubit channel differs from that of the broadband bosonic channel by a constant of order unity.

Note, as above, that the energy applied during transmission need not be dissipated: it is merely the energy invested in the propagation of information and can in principle be recovered after transmission. In fact, existing quantum logic devices can swap information from one place to another at rates approaching C_{1q}, with minimal dissipation during the transfer process.

A simple example of an interaction that attains the qubit capacity limit C_{1q} is the application of a 'swap' operation: $S|\psi\rangle_A|\phi\rangle_B = |\phi\rangle_A|\psi\rangle_B$ for all $|\psi\rangle, |\phi\rangle$. Clearly, the swap operator performs the desired transfer, and as shown in Ref. 29, attains the power/capacity limit of the qubit channel. It does so coherently and without dissipation in principle. As noted above, existing quantum logic devices can swap information from one place to another at rates very close to this limit.[35–38]

The proof that swap attains the desired limit C_{1q} relies on the properties of the swap operator:[29] S is unitary, $S^2 = 1$, consequently S is also Hermitian, $S = S^\dagger$. It is straightforward to show that $e^{i\pi S/2} = iS$. The proof that swap attains the desired power-limited information transfer rate for the qubit channel uses S as a Hamiltonian, and applies this Hamiltonian for a time necessary to effect the information transfer.

The 'swap' picture of quantum information transmission assumes a direct transfer of A's qubit to B over a time $\Delta t \geq d(AB)/c$, where $d(AB)$ is the distance between A and B. To look at propagation effects, consider the case in which A's and B's qubits are coupled by an intervening chain of qubits $A_1 B_1 A_2 B_2 \ldots A_n B_n$, where A has access to A_1 and B has access to B_n. Here, it can be shown[29] that the transmission of information from A to B by repeated swapping down the chain of qubits comes within $\sqrt{2}$ of the power/capacity limit C_{1q}.

Now turn to 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 amongst the channels.[1] Each channel now transmits at a rate $(2/\sqrt{\pi})\sqrt{P/M\hbar}$ giving an overall rate of transmission $C_{Mc} = (2M/\sqrt{\pi})\sqrt{P/Mh} = (2/\sqrt{\pi})\sqrt{MP/h} = \sqrt{M} C_{1q}$. This rate enhancement is the best known enhancement for parallel unentangled channels and holds for both the bosonic channel and for the qubit channel. Because of the square root dependence of transmission rate on power, both the qubit and broadband bosonic channel are more efficient at a lower power. As a result, one improves performance by dividing up information and power among the different channels.

Now we show that one can improve on the unentangled transmission rate C_{Mc} by engineering interactions that entangle the qubit channels in the process of transmission. The goal of the M-channel transfer is to enact the $2M$-qubit analog of the swap above: $S_{1\ldots M} = S_1 S_2 \ldots S_M$, 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.). An obvious way to perform the $2M$-qubit swap is just to apply M two-qubit swaps, i.e., one applies the Hamiltonian $S_1 + S_2 + \ldots + S_M$ for an amount of time required to perform the transfer in each of the channels. Since $e^{i\pi(S_1+S_2+\ldots+S_M)/2} = i^M S_1 S_2 \ldots S_M$, this method clearly effects the transfer. It is straightforward to verify that this method attains the unentangled transfer limit C_{Mq} above.

But the unentangled limit can be surpassed by the following method. $S_{1\ldots M}$ is Hermitian and can be applied as a Hamiltonian. It is easy to verify that $e^{i\pi S_{1\ldots M}/2} = iS_{1\ldots M}$: accordingly, applying the $2M$-qubit swap operator as a Hamiltonian also swaps the qubits. In addition, it does so more efficiently than swapping the qubits one by one. In fact, in Ref. 29 it is shown that the transmission rate for applying the $2M$-qubit swap Hamiltonian is $C_{Mq} = 1/\Delta t = \sqrt{2(1-2^{-M})P/\pi\hbar}$. Comparing C_{Mq} with C_{Mc} we see that using the $2M$-qubit swap operator as a Hamiltonian gives an enhancement in transmission rate of $\sqrt{M}$ over swapping the qubits one by one.

In addition, applying the Hamiltonian $S_{1\ldots M}$ necessarily entangles the M qubit channels (except in some very simple cases as when the message being transmitted is $00\ldots0$). 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 $(e^{-i\pi/4}/\sqrt{2})\big(|b_1 \ldots b_M\rangle_A |00\ldots0\rangle_B + i|00\ldots0\rangle_A |b_1 \ldots b_M\rangle_B\big)$. Transferring M bits down M uncoupled, unentangled quantum channels using the same power as a single qubit channel takes $\sqrt{M}$ times longer than transferring the information down coupled, entangled channels. Unentangled transfer corresponds to the application of M two-qubit swap operations with Hamiltonian $S_1 + \ldots S_M$ as opposed to the $2M$-qubit swap Hamiltonian $S_{1\ldots M} = S_1 S_2 \ldots S_M$, 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.

The use of entanglement allows the transfer of M bits in the same time and using the same power that it takes to transfer a single bit. In some 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 π radians apart in angle. 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 one bit. Effectively, the coupling between the channels allows them to transmit information in the form a 'super-boson' 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[32] and quantum positioning.[33]

Of course, enacting the necessary Hamiltonian $\tilde{S}_{1\ldots M}$ is likely to prove experimentally difficult. 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 can be written $S = \sigma_x^A \sigma_x^B + \sigma_y^A \sigma_y^B + \sigma_z^A \sigma_z^B$, 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, and corresponds 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.

The results presented here represent an extension of concepts of quantum information processing to enhancing the power-limited capacity of communication channels using entanglement. The use of entanglement and squeezing to improve the efficiency of power-limited systems appears to be a generic feature of quantum mechanics. Database search, interferometry, quantum clocks, the accuracy of positioning and lithography, and now the capacity of quantum channels, all receive a benefit of $\sqrt{M}$ by using squeezing and entanglement. It is interesting to speculate what other quantum technologies might so benefit. The strength of quantum materials? The power of quantum heat engines? Time will tell.

Acknowledgments

This work was funded by ARDA, NRO, and ARO under a MURI program.

References

1. C. M. Caves and P. D. Drummond, *Rev. Mod. Phys.* **66**, 481-537 (1994).
2. J. P. Gordon, in *Advances in Quantum Electronics*, J. R. Singer ed., (Columbia, New York, 1961), p. 509.
3. D. S. Lebedev and L. B. Levitin, *Dok. Akad. Nauk SSSR* **149**, 1299; *Sov. Phys. Dokl.* **8**, 377 (1963).
4. D. S. Lebedev and L. B. Levitin, *Inf. Control* **9**, 1 (1966).
5. H. Marko, *Kybernetik* **2**, 274 (1965).
6. H. Takahasi, in *Advances in Communication Systems, Vol. 1*, A. V. Balakrishnan, ed., (Academic, New York 1965), p. 227.
7. J. I. Bowen, *IEEE Trans. Inf. Theory* **IT-13**, 230 (1967).
8. R. Landauer and J. W. F. Woo, in *Synergetics*, H. Haken, ed., (Tuebner, Stuttgart 1973), p. 97.
9. C. W. Helstrom, *Proc. IEEE* (Lett.) **62**, 139 (1974).
10. H. P. Yuen and J. H. Shapiro, *IEEE Trans. Inf. Theory* **IT-24**, 657 (1978).
11. J. H. Shapiro, H. P. Yuen, and J. A. Machado Mata, *IEEE Trans. Inf. Theory* **IT-25**, 179 (1979).
12. H. P. Yuen and J. H. Shapiro, *IEEE Trans. Inf. Theory* **IT-26**, 78 (1980).
13. L. B. Levitin, *Int. J. Th. Phys.* **21**, 299 (1982).
14. J. B. Pendry, *J. Phys. A* **16**, 2161 (1983).
15. Y. Yamamoto and H. A. Haus, *Rev. Mod. Phys.* **58**, 1001 (1986).
16. B. E. A. Saleh and M. C. Teich *Phys. Rev. Lett.* **58** 2656 (1987).
17. R. Landauer, *Nature* **335**, 779 (1988).
18. J. D. Bekenstein, *Phys. Rev. A* **37**, 3437 (1988).
19. J. D. Bekenstein and M. Schiffer, *Int. J. Mod. Phys. C* **1**, 355 (1990).

20. M. Schiffer, *Phys. Rev. A* **43**, 5337 (1991).
21. H. P. Yuen and M. Ozawa, *Phys. Rev. Lett.* **70**. 363 (1992).
22. B. E. A. Saleh and M. C. Teich, *Proc. IEEE* **80**, 451 (1992).
23. A. S. Kholevo, *Probl. Peredachi Inf.* **9**, 3 (1973) [*Probl. Inf. Transm. (USSR)* **9**, 177 (1973)].
24. E. H. Lieb and M. B. Ruskai, *J. Math. Phys.* **14**, 1938 (1973).
25. C. H. Bennett and S. J. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992).
26. B. Schumacher and M. D. Westmoreland, *Phys. Rev. A* **56**, 131 (1997).
27. A. S. Holevo, *IEEE Trans. Inf. Theory* **44**, 269 (1998).
28. C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliy, 'Entanglement-Assisted Capacity of a Quantum Channel and the Reverse Shannon Theorem,' quant-ph/0106052.
29. S. Lloyd, *The power of entangled quantum channels,* submitted to Nature, quant-ph/0112034.
30. A. Peres, *Quantum Theory: Concepts and Methods*, (Kluwer, Hingham) 1995.
31. N. Margolus and L B. Levitin, in *PhysComp96*, T. Toffoli, M. Biafore, J. Leao, eds. (NECSI, Boston) 1996; *Physica D* **120**, 188-195 (1998).
32. L. K. Grover, in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, ACM Press, New York, 1996, pp. 212-218.
33. V. Giovannetti, S. Lloyd, and L. Maccone, *Nature* (2001).
34. Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, *Phys. Rev. Lett.* **75**, 4710-4713 (1995).
35. C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, *Phys. Rev. Lett.* **75**, 4714-4717 (1995).
36. D. G. Cory, A. F. Fahmy, and T. F. Havel, in *PhysComp96, Proceedings of the Fourth Workshop on Physics and Computation*, T. Toffoli, M. Biafore, J. Leão, eds., (New England Complex Systems Institute, Boston) 1996.
37. N. A. Gershenfeld and I. L. Chuang, *Science* **275**, pp. 350-356 (1997).