# The Structure of Quantum Information

Christopher A. Fuchs
*Norman Bridge Laboratory of Physics 12-33,*
*California Institute of Technology, Pasadena CA 91125*
(5 November 1998)

1998 PACS numbers: 03.67.-a, 03.67.Dd, 03.67.Lx, 03.67.Hk, 02.50.-r, 02.50.Le, 02.10.Sp, 05.30.-d, 03.65.Bz

## I. ORIENTATION

The world we live in is well-described by quantum mechanics. What should we make of that? In a way, the answer to this question was once less positive than it is today. For although quantum theory is a tool of unprecedented accuracy in predicting and controlling the phenomena about us—and by way of that is the basis of our technological society—the intellectual lesson we have come to derive from it has been one largely of limitations. The best place to see this attitude at work is in a standard presentation of the Heisenberg uncertainty relations. It is almost as if the world were holding something back that we really had every right to possess: the task of physics, or so it was believed, is simply to sober up to this fact and make the best of it.

In contrast to this textbook lesson, the last five years have seen the start of a significantly more positive, almost intoxicating, attitude about the basic role of quantum mechanics. This is evidenced no more clearly than within the small, but growing [1], community of workers in *Quantum Information Theory* [2] and *Quantum Computing* [3].[1] The point of departure in both these disciplines is not to ask what limits quantum mechanics places upon us, but instead what novel, productive things we can do in the quantum world that we could not have done otherwise. In what ways can we say that the quantum world is fantastically better than the classical world?

The two most striking examples of this so far have been quantum cryptographic key distribution [4,5] and Shor's quantum factoring algorithm [6,7]. In the case of the first example, one sees that quantum mechanics allows two communicators to transmit to each other a random cryptographic key in such a way that eavesdropping on the transmission can be excluded out of hand. This is impossible in the classical world because there is no direct connection between the information that can be gathered about a physical system's state and the disturbances induced upon that state in the process [8,9]. Without the indeterminism of quantum mechanics, two-party data transmissions would remain forever vulnerable to clever or powerful eavesdropping techniques.

In the case of the second example, one sees that algorithms designed for computers built of unabashedly quantum components—that is, components that can remain coherent with each other throughout the computation—can factor large integers exponentially faster than anything written for standard classical computers. To give a quick example of what this means in real terms, consider a 600-digit number that is known to be the product of two (secret) primes. The number of computational steps required of a classical computer to crack it into its two components is of the order of $10^{34}$. In contrast, the corresponding number of steps for a quantum computer is only $10^{11}$. Quantum computing can give 23 orders of magnitude greater efficiency in this problem!

These two examples are the most outstanding of the class, and there is well-founded hope that they are the tip of a technological iceberg. However, I believe there is a similarly founded hope that they are also the small tip of a *physical* iceberg. Looking at quantum mechanics through the eyes of these two fields cannot help but lead to greater and deeper—and perhaps the deepest—insights into its structure and ultimate use. These are the insights that could poise physics for the great breakthroughs that will surely come about next century, even in disciplines as far-flung as quantum gravity and quantum cosmology.

But this is my grand vision. Little will come of it if it is not preceded by years of more realistic, more concrete exploration of the *structure of quantum information.* This, as part of the accumulating results of the communities just described, is the subject of this research proposal.

To give some indication of the wider context that flows into the specialization of Quantum Information and Quantum Computing, one need only note that, by its very makeup, it must call upon the expertise of standard communication theory, cryptography, computation theory, number theory, signal processing, and various branches of statistical mechanics. Dreams of possible experimental implementations have called upon the quantum optics community [10,11], the ion trap community

[1] For quick reference, two recent articles on the subject can be found in *Physics Today*: Oct. 1997, pp. 19–21, and Oct. 1995, pp. 24–30. Some WWW links can be found in John Preskill's "Physics 229" homepage at `http://www.theory.caltech.edu/people/preskill/ph229`. Also see Oxford University's Centre for Quantum Computation homepage at `http://www.qubit.org/`.

[12,13], the NMR spectroscopy community [14,15], and to a smaller extent solid-state physics [16,17].

The particular aspect of Quantum Information Theory that has been my focus the last four years is closely allied to the well-established tradition in mathematical physics pioneered by the likes of Holevo [18], Lieb [19], Lindblad [20], and Uhlmann [21]. It is my intent to strengthen and build upon the connections between that tradition and this upstart field, which already in many ways is its continuation. I hope this becomes apparent in the details that follow.

## II. RESEARCH PROPOSAL

My research interests might be described as *tria juncta in uno*.[2] The conjunction of these three topics, for the most part, exhausts what is presently meant by "Quantum Information Theory."

• **Sending Classical Information on Quantum Mechanical Channels.** People encode "classical" information—like the stories in today's newspaper—into the states of quantum systems for a simple reason: to get it from one place to another. Since the world is quantum mechanical, this, in the last analysis, is exactly what one always does in transmitting information. Strangely enough however, literally almost all of modern information theory (as exhibited in the 44 existent volumes of *IEEE Transactions on Information Theory*) has ignored this fact in any but the most trivial ways.

Once one takes it seriously that physical information carriers are quantum mechanical, one can ask a whole host of questions that could not have been asked before. For instance, can it help the receiver to collect many separate transmissions before performing the quantum measurement required to decode them [22,23]? That is to say, can collective quantum measurements on separate signals be more powerful than individual measurements [24,25]? Can it ever help to entangle separate transmissions—as with Einstein-Podolsky-Rosen pairs—before sending them through the channel [26]? Can one help evade a channel's noise by encoding the signals in nonorthogonal quantum states [27,28], in spite of the fact that the classical analog of this corresponds to sending noisy signals?

Of course, the answer to all these questions is "yes." And this is enough to demonstrate that these lines of thought are not trivial. However, the work remaining before a theory as coherent as classical information theory can emerge is legion. In particular, the counterpart of the most basic question of all classical information theory—What is the capacity of a discrete memoryless channel?—has yet to be solved.

The most exciting prospect of this set of questions for physics is the potential it holds for giving new and unique and very strongly motivated measures of "correlation" between two subsystems of a larger whole. Shannon's solution of the channel capacity question brought with it a measure of correlation (the "mutual information") of a generality greatly exceeding the scope of its motivation [29]. Its physical applications have ranged from information theoretic versions of the Heisenberg relations [30] to a final solution of the old Maxwellian demon problem [31,32]. One can expect no less for a quantum measure of classical correlation. In particular, the importance of uniquely quantum measures of correlation for quantum statistical mechanics has been emphasized recently by Lindblad [33] and Schack and Caves [34].

• **Information Gain vs. Quantum State Disturbance in Quantum Theory.** The engine that powers quantum cryptography is the principle that it is impossible to gather information about a quantum system's unknown state without disturbing that system in the process. (This is so even when the state is assumed to be one of only two nonorthogonal possibilities.) This situation is often mistakenly described as a consequence of the "Heisenberg uncertainty principle" but, in fact, is something quite distinct [8,9] and only now starting to be studied in the physical literature. A more accurate account of the principle is that it is a feature of quantum mechanics that rests ultimately on the unitarity of the theory, and may be seen as a quantitative extension of the so-called "no-cloning theorem" [35–37]. In contradistinction, the Heisenberg principle concerns our inability to "get hold" of two classical observables—such as a position and momentum—simultaneously. It thus concerns our inability to ascribe *classical* states of motion to *quantum* systems—that has very little to do with the issue of encoding information in and retrieving information from the quantum states themselves.

Because this way of looking at "information gain" and "disturbance" for quantum systems is itself purely quantum mechanical and does not rely on antiquated classical notions, it holds the possibility of giving the best understanding yet of those things the founding fathers (like Heisenberg, Pauli, and Bohr) labored so hard to formulate. But what is the unifying theme? What are the directions to take? One can elaborate upon the direction defined by practical quantum cryptography [38–40] or one can take a more direct route inspired by the original no-cloning theorem [41–43]. Each method is begging for a more systematic account than has been afforded by these simple preparatory explorations.

A novel approach, and one which I have turned my attention to recently, is to seek out the connection between quantum entanglement measures and the information–disturbance principle [43–45]. The main point about this line of thought is that in the scenario of quantum cryp-

[2] Not to worry, I won't pretend that I knew this phrase before looking in my thesaurus! ... But when you learn something like this, you've just got to use it! Apparently this phrase is the motto of "The Most Honourable Order of the Bath," a particular British order of chivalry.

tography, any would-be eavesdroppers must become entangled with the information carriers traveling between the legitimate users. Can one read the tradeoff between information and disturbance directly from something to do with entanglement itself? Perhaps by a sort of "entanglement conservation" principle? These are the sorts of questions that first require progress in the next research topic.

• **Quantifying Quantum Entanglement: Separating It from Classical Correlation.** The preoccupation of classical information theory is to make the correlation between sender and receiver as high as possible. This is what communication is about. But it is only part of the story in Quantum Information Theory. The quantum world brings with it a new resource that senders and receivers can share: quantum entanglement, the stuff Einstein-Podolsky-Rosen pairs and Bell-inequality violations are made of. This new resource, of all the things mentioned so far, is the most truly "quantum" of quantum information. It has no classical analog, nor might it have been imagined in a classical world.

What is quantum entanglement? It is *not* probabilistic correlation between two parts of a whole. Rather it is the *potential* for such a correlation. In a quick portrayal:

*classical correlation*—

> Alice and Bob entered a lottery for which they were the only players. They have not opened their "winnings" envelopes yet, but the messages in them say that one is the winner and one is the loser. Which is which, they do not know—they only know the correlation—but the answer is there, objectively existent, without their looking.

*quantum entanglement*—

> Alice and Bob will eventually perform measurements on the EPR pair their envelopes contain and the outcomes *will* be correlated. However, before the measurements are performed, there are no objectively existent variables already there. Different measurements can and will lead to different correlations.

In a certain sense, entanglement is a kind of *all-purpose correlation* just waiting to be baked into something real—a quantum "Martha White's Flour" [46]. The uses for this all-purpose correlation are manifold within Quantum Information Theory. Beside the applications above [4,26], there is also quantum-state teleportation [47], quantum superdense coding [48,49], error-correction for quantum computers [50], entanglement-assisted multi-party communication games [51], better control of atomic frequency standards [52,53], and the list goes on.

The deepest set of questions here, and the largest focus of my present research [54,55], concern quantifying this newly recognized physical essence in an application-independent way [56–58]. As an example, take an EPR pair, half of which has been transmitted through a noisy (decohering) quantum channel. Because of the noise, the final state of this bipartite system is no longer a pure state: it is described by a mixed state density operator. Some of the correlation there is still potential or all-purpose, but some—because the decoherence has helped promote it to a more tangible status—is simply classical correlation. How do we quantify the amount of each? What, if anything, is the exchange rate between the two? With some time, creativity, and hard work, we will one day have these issues under control.

•• **Synthesis.** In some ways the project of Quantum Information Theory can be likened to the beginning of thermodynamics. It is not our place to develop the question "What is heat, work, energy?" but instead "What is correlation, indeterminism, entanglement?" No informed judgment of the historic question could have been made before the development of a quantitative theory of thermodynamics, and it will be likewise with our field. Whereas the fruits of the old question were the mechanical theory of heat and its corollary of atomism, we do not yet have a firm grasp of where our field is leading. It is clear, however, that it is going somewhere and somewhere fast; at the very least, its applied, technological innovations can neither be denied nor safely ignored.

What is correlation, indeterminism, entanglement? This is what the three research areas above are trying to make quantitative. Each contains within itself a little seed of the others; each sheds light on the structure of quantum information.

## III. WIDER SEAS

Eight years after the inception of classical information theory, Claude Shannon, its founder, warned [59],

> Although this wave of popularity is ... pleasant and exciting for those of us working in the field, it carries at the same time an element of danger. While we feel that information theory is a valuable tool in providing fundamental insights into the nature of communication ... it is certainly no panacea .... Seldom do more than a few of nature's secrets give way at one time.

History has borne Shannon out: information theory is not a panacea. But, cure-all or not, the field has had a great impact on applications that can hardly be said to resemble the original one, that of describing communication over noisy channels [60]. One need only look at information theory's influence on fields as far ranging as biology, economics, and psychology [61], to see this point.

What is it that we can expect of *Quantum* Information Theory once it is complete and coherent? What more might it say about a *few* of natures secrets? With the reader's indulgence, I will attempt to express some of my present views on the question. These have to do with the "grand vision" and "physical iceberg" of the Introduction—the real sources of my day-to-day motivation.

The year 1957 is significant in physical thought because it marks the penetration of information theory into physics in a systematic way—into statistical mechanics in particular [62]. This refers to the *Maximum Entropy* or "MaxEnt" program for statistical mechanics set into motion by E. T. Jaynes [63]. With the tools of information theory, one was able for the first time to make a clean separation between the purely *statistical* and the purely *physical* aspects of the subject matter.

Perhaps it would be good to present a mild example of this. Because of MaxEnt, a standard statistical mechanical ensemble—like the canonical ensemble—can finally be seen for what it really is: an expression of the physicist's *state of knowledge* (specified, of course, by the experimental parameters under his control). Though this reveals a subjective element in statistical mechanics, the ensemble is not arbitrary. Two physicists working on a single experiment and possessing identical data—if true to their states of knowledge—will derive the same distributions for the system's variables. The *structure* of the canonical distribution, with its exponential form, is due purely to the kind of knowledge the experimenter possesses—in this particular case, the expectation value of some observable and nothing else. That is to say, the canonical distribution's form is a theorem of the laws of inference, *not physics.* The physics of the system rests solely in its Hamiltonian and boundary conditions. This conceptual separation between the physical and the statistical can be fruitful. With it, one can, for instance, derive the second law of thermodynamics in an almost trivial way [64].

In contrast to this, quantum theory is at its heart a statistical theory of *irreducibly* statistical phenomena—this is the great lesson of the Kochen-Specker theorems and the Bell inequalities [66]. What can this possibly mean for the issue just explored? With due attention to the success of the MaxEnt program in the last 40 years [65], one can hardly feel it unreasonable to ask: What part of the formal structure of quantum mechanics is forced upon us by physics alone—i.e., that the theory be about irreducibly statistical phenomena—and what part is forced upon us as a consequence of the form *any* theory must take in light of that subject matter [67,68]? George Boole called probability theory a "law of thought" because it specifies the rules with which we should think when we come upon situations where our information is incomplete [69,70]. What part of quantum mechanics is simply "law of thought," and what part is *irreducibly* physics?

A mature Quantum Information Theory is likely to be uniquely stationed to contribute to this question, or at least to test whether anything might come of it. The quantitative statements it *will* possess for the information–disturbance tradeoff and the correlation–entanglement dichotomy should be of just the right flavor for such a thing. Both threads explore the difference between probabilities that can be improved upon because they correspond to lack of knowledge and probabilities that are more the nature of "potentialities" for which no improvement can be had.

Once this issue is settled, one may finally hope for a simple, crisp statement of what our quantum theory is all about [71]. And once that is in hand, who knows what the limits might be? To place the issue within an historical context, one can speculate how long it would have taken to stumble across general relativity if it had not been for the compelling vision that Einstein found lying behind the Lorentz transformations. The equations were there with Lorentz, but the essence of it all—and the simple picture with which progress could be made—came with Einstein's special relativity.

Comparable to this opportunity for fundamental physics, one might imagine a similar blossoming of opportunity for other endeavors. A classification of quantum theory's content in the way suggested above could distill mathematical structures that other, extra-quantum-mechanical, efforts [72–74] might use to their advantage. After all, this is exactly the sort of thing that happened with the MaxEnt program: its applications range from observational astronomy to pharmaceutical studies to artificial intelligence[3] [63]. Are there fields beside quantum physics that encounter situations where the maximal knowledge of something can never be made deterministically complete [75–77]? If so, then they will plausibly find novel use for the *mathematics*[4] of quantum physics and Quantum Information Theory.

The main point that I would like to impress with this final speculation—even allowing that the details above be taken with a grain of salt—is that the structure of quantum mechanics is an amazingly beautiful intellectual edifice. It would be a shame if its only application were for quantum mechanics itself.

## IV. SUMMARY

There is a grand adventure in front of the physics community called Quantum Information and Quantum Computing. Its hallmark is to view quantum theory in a way little before explored, in a way that accentuates the positive. Delimiting the structure of quantum information may well be a key to great progress in fundamental physics—but that may be some time in the coming. In the mean time there is much solid work to be done exploring entanglement, information vs. disturbance, and the information-carrying capacities of quantum mechanical systems. This is my preoccupation; this is the field of research I call my home. I thank you for your consideration.

[3] A particularly cogent example of the use of these methods in artificial intelligence can be found at Microsoft Research Division's *Decision Theory & Adaptive Systems Group* homepage: `http://www.research.microsoft.com/dtas/`.

[4] Please note that I *did* say "the mathematics of" here.

* *Note 1*: This bibliography makes no attempt to be complete or to consistently cite original references. Its main purpose is to give the reader a more detailed introduction to the issues discussed in this text.

* *Note 2*: All "LANL e-print" listings refer to the Los Alamos National Laboratory E-print Archive at `http://xxx.lanl.gov`.

[1] G. Taubes, "All Together for Quantum Computing," Science **273**, 1164 (1996).

[2] C. H. Bennett, "Quantum Information and Quantum Computation," Phys. Tod. **48**, No. 10, 24 (1995).

[3] A. M. Steane, "Quantum Computing," Rep. Prog. Phys. **61**, 117 (1998).

[4] C. H. Bennett, G. Brassard, and A. K. Ekert, "Quantum Cryptography," Sci. Am. **267**, No. 10, 50 (1992).

[5] A. Muller, H. Zbinden, and N. Gisin, "Underwater Quantum Coding," Nature **378**, 449 (1995).

[6] D. P. DiVincenzo, "Quantum Computation," Science **270**, 255 (1995).

[7] A. Ekert and R. Jozsa, "Quantum Computation and Shor's Factoring Algorithm," Rev. Mod. Phys. **68**, 733 (1996).

[8] C. A. Fuchs and A. Peres, "Quantum State Disturbance vs. Information Gain: Uncertainty Relations for Quantum Information," Phys. Rev. A **53**, 2038 (1996).

[9] C. A. Fuchs, "Information Gain vs. State Disturbance in Quantum Theory," Fortschr. Phys. **46**, 535 (1998).

[10] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, "Measurement of Conditional Phase Shifts for Quantum Logic," Phys. Rev. Lett. **75**, 4710 (1995).

[11] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, "Unconditional Quantum Teleportation," Science **282**, 706 (1998).

[12] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, "Demonstration of a Universal Quantum Logic Gate," Phys. Rev. Lett. **75**, 4714 (1995).

[13] R. J. Hughes, et al., "The Los Alamos Trapped Ion Quantum Computer Experiment," Fortschr. Phys. **46**, 329 (1998).

[14] D. G. Cory, A. F. Fahmy, and T. F. Havel, "Ensemble Quantum Computing by NMR Spectroscopy," Proc. Natl. Acad. Sci. USA **94**, 1634 (1997).

[15] N. A. Gershenfeld and I. L. Chuang, "Bulk Spin-Resonance Quantum Computation," Science **275**, 350 (1997).

[16] D. Loss and D. P. DiVincenzo, "Quantum Computation with Quantum Dots," Phys. Rev. A **57**, 120, (1998).

[17] B. E. Kane, "A Silicon-Based Nuclear Spin Quantum Computer," Nature **393**, 133 (1998).

[18] A. S. Holevo, "Statistical Decision Theory for Quantum Systems," J. Multivar. Anal. **3**, 337 (1973).

[19] E. H. Lieb, "Convex Trace Functions and the Wigner-Yanase-Dyson Conjecture," Adv. Math. **11**, 267 (1973).

[20] G. Lindblad, "On the Generators of Quantum Dynamical Semigroups," Comm. Math. Phys. **48**, 119 (1976).

[21] A. Uhlmann, "The 'Transition Probability' in the State Space of a $^*$-algebra," Rep. Math. Phys. **9**, 273 (1976).

[22] A. S. Holevo, "The Capacity of Quantum Communication Channel with General Signal States," IEEE Trans. Inf. Theor. **44**, 269 (1998).

[23] B. Schumacher and M. D. Westmoreland, "Sending Classical Information via Noisy Quantum Channels," Phys. Rev. A **56**, 131 (1997).

[24] A. S. Kholevo, "On the Capacity of Quantum Communication Channel," Prob. Inf. Transm. **15**, 247 (1979).

[25] A. Peres and W. K. Wootters, "Optimal Detection of Quantum Information," Phys. Rev. Lett. **66**, 1119 (1991).

[26] C. H. Bennett, C. A. Fuchs, and J. A. Smolin, "Entanglement-Enhanced Classical Communication on a Noisy Quantum Channel," in *Quantum Communication, Computing and Measurement*, edited by O. Hirota, A. S. Holevo, and C. M. Caves (Plenum, New York, 1997).

[27] C. A. Fuchs, "Nonorthogonal Quantum States Maximize Classical Information Capacity," Phys. Rev. Lett. **79**, 1163 (1997).

[28] C. A. Fuchs, P. W. Shor, J. A. Smolin, and B. M. Terhal, "Quantum-Enhanced Classical Communication," to be submitted to Phys. Rev. A; preliminary draft available upon request.

[29] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, (John Wiley & Sons, New York, 1991).

[30] M. J. W. Hall, "Information Exclusion Principle for Complementary Observables," Phys. Rev. Lett. **74**, 3307 (1995).

[31] C. H. Bennett, "The Thermodynamics of Computation—a Review," Int. J. Theo. Phys. **21**, 905 (1982).

[32] W. H. Zurek, "Algorithmic Randomness and Physical Entropy," Phys. Rev. A **40**, 4731 (1989).

[33] G. Lindblad, "Quantum Entropy and Quantum Measurements," in *Quantum Aspects of Optical Communications*, edited by C. Bendjaballah, O. Hirota, and S. Reynaud (Springer-Verlag, Berlin, 1991).

[34] R. Schack and C. M. Caves, "Information-Theoretic Characterization of Quantum Chaos," Phys. Rev. E **53**, 3257 (1996).

[35] W. K. Wootters and W. H. Zurek, "A Single Quantum Cannot Be Cloned," Nature **299**, 802 (1982).

[36] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum Cryptography Without Bell's Theorem," Phys. Rev. Lett. **68**, 557 (1992).

[37] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, "Noncommuting Mixed States Cannot Be Broadcast," Phys. Rev. Lett. **76**, 2818 (1996).

[38] C. A. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres, "Optimal Eavesdropping in Quantum Cryptography. I. Information Bound and Optimal Strategy," Phys. Rev. A **56**, 1163 (1997).

[39] B. A. Slutsky, R. Rao, P.-C. Sun, and Y. Fainman, "Security of Quantum Cryptography Against Individual Attacks," Phys. Rev. A **57**, 2383 (1998).

[40] J. I. Cirac and N. Gisin, "Coherent Eavesdropping Strategies for the 4-State Quantum Cryptography Pro-

tocol," Phys. Lett. A **229**, 1 (1997).

[41] V. Bužek and M. Hillery, "Quantum Copying: Beyond the No-Cloning Theorem," Phys. Rev. A **54**, 1844 (1996).

[42] N. Gisin and S. Massar, "Optimal Quantum Cloning Machines," Phys. Rev. Lett. **79**, 2153 (1997).

[43] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, "Optimal Universal and State-dependent Quantum Cloning," Phys. Rev. A **57**, 2368 (1998).

[44] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum Privacy Amplification and the Security of Quantum Cryptography Over Noisy Channels," Phys. Rev. Lett. **77**, 2818 (1996).

[45] B. Schumacher and M. D. Westmoreland, "Quantum Privacy and Quantum Coherence," Phys. Rev. Lett. **80**, 5695 (1998).

[46] L. Flatt and E. Scruggs, "The Martha White Theme," on *Flatt & Scruggs: 1948–1959* (Bear Family Records, 1994).

[47] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels," Phys. Rev. Lett. **70**, 1895 (1993).

[48] C. H. Bennett and S. J. Wiesner, "Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States," Phys. Rev. Lett. **69**, 2881 (1992).

[49] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, "Dense Coding in Experimental Quantum Communication," Phys. Rev. Lett. **76**, 4656 (1996).

[50] D. Gottesman, *Stabilizer Codes and Quantum Error Correction*, Ph. D. Thesis, California Institute of Technology, 1997; LANL e-print `quant-ph/9705052`.

[51] R. Cleve and H. Buhrman, "Substituting Quantum Entanglement for Communication," Phys. Rev. A **56**, 1201 (1997).

[52] J. J. Bollinger, W. M. Itano, D. J. Wineland, and D. J. Heinzen, "Optimal Frequency Measurements with Maximally Correlated States," Phys. Rev. A **54**, R4649 (1996).

[53] S. F. Huelga, C. Macchiavello, T. Pellizzari, A. K. Ekert, M. B. Plenio, and J. I. Cirac, "On the Improvement of Frequency Stardards with Quantum Entanglement," Phys. Rev. Lett. **79**, 3865 (1997).

[54] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, "Quantum Nonlocality without Entanglement" Phys. Rev. A **59**, ?? (1999); LANL e-print `quant-ph/9804053`.

[55] D. P. DiVincenzo, C. A. Fuchs, H. Mabuchi, J. A. Smolin, A. Thapliyal, and A. Uhlmann, "Entanglement of Assistance," to appear in *The 1st NASA International Conference on Quantum Computing & Quantum Communications (NASA QCQC'98)*, edited by C. Williams (Springer-Verlag, Berlin, 1998); LANL `quant-ph/9803033`.

[56] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels," Phys. Rev. Lett. **76**, 722 (1996).

[57] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed State Entanglement and Quantum Error Correction," Phys. Rev. A **54**, 3825 (1996).

[58] W. K. Wootters, "Entanglement of Formation of an Arbitrary State of Two Qubits," Phys. Rev. Lett. **80**, 2245 (1998).

[59] C. E. Shannon, "The Bandwagon," IEEE Trans. Inf. Theor. **IT-2**, No. 3, 3 (1956).

[60] C. E. Shannon, "A Mathematical Theory of Communication," Bell Sys. Tech. J. **27**, 379, 623 (1948).

[61] J. Campbell, *Grammatical Man: Information, Entropy, Language, and Life*, (Simon & Schuster, New York, 1982).

[62] E. T. Jaynes, "Information Theory and Statistical Mechanics," Phys. Rev. **106**, 620 (1957).

[63] A convenient source of information about this program can be found in the dozen or so conference proceedings all published under the same title, *Maximum Entropy and Bayesian Methods* (Kluwer, Dordrecht).

[64] E. T. Jaynes, "Gibbs vs. Boltzmann Entropies," Am. J. Phys. **33**, 391 (1965).

[65] E. T. Jaynes, "Where Do We Stand on Maximum Entropy?," in *The Maximum Entropy Formalism*, edited by R. D. Levine and M. Tribus (MIT Press, Cambridge, MA, 1979).

[66] N. D. Mermin, "Hidden Variables and the Two Theorems of John Bell," Rev. Mod. Phys. **65**, 803 (1993).

[67] C. M. Caves and C. A. Fuchs, "Quantum Information: How Much Information in a State Vector?," in *The Dilemma of Einstein, Podolsky and Rosen – 60 Years Later*, edited by A. Mann and M. Revzen, Ann. Israel Phys. Soc. **12**, 226 (1996).

[68] C. M. Caves, C. A. Fuchs and R. Schack, "Bayesian Probability in Quantum Mechanics," to be submitted to Am. J. Phys. Preliminary draft available upon request.

[69] G. Boole, *An Investigation of the Laws of Thought*, (Dover, New York, 1958).

[70] E. T. Jaynes, *Probability Theory: The Logic of Science.* This massive book was unfortunately not completed before Prof. Jaynes' death. Preprints are available at `http://bayes.wustl.edu/`.

[71] C. Rovelli, "Relational Quantum Mechanics," Int. J. Theor. Phys. **35**, 1637 (1996).

[72] I. Pitowski, "From George Boole to John Bell—The Origins of Bell's Inequality," in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, edited by M. Kafatos (Kluwer, Dordrecht, 1989).

[73] I. Pitowski, "George Boole's 'Conditions of Possible Experience' and the Quantum Puzzle," Brit. J. Phil. Sci. **45**, 95 (1994).

[74] W. Segal and I. E. Segal, "The Black-Schole Pricing Formula in the Quantum Context," Proc. Natl. Acad. Sci. USA **95**, 4072 (1998).

[75] S. Watanabe, "A Model of Mind-Body Relation in Terms of Modular Logic," Synthese **13**, 261 (1961).

[76] A. Peres and W. H. Zurek, "Is Quantum Theory Universally Valid?," Am. J. Phys. **50**, 807 (1982).

[77] J. L. Heilbron, *The Dilemmas of an Upright Man: Max Planck as Spokesman for German Science*, (U. California Press, Berkeley, 1986), pp. 127–128.