

# Quantum information and physics: some future directions\*

John Preskill,<sup>†</sup>

*Lauritsen Laboratory of High Energy Physics  
California Institute of Technology  
Pasadena, CA 91125, USA*

(April, 1999)

I consider some promising future directions for quantum information theory that could influence the development of 21st century physics. Advances in the theory of the distinguishability of superoperators may lead to new strategies for improving the precision of quantum-limited measurements. A better grasp of the properties of multi-partite quantum entanglement may lead to deeper understanding of strongly-coupled dynamics in quantum many-body systems, quantum field theory, and quantum gravity.

## I. INTRODUCTION

With the discovery of an apparent separation between the classical and quantum classifications of computational complexity [1], and of fault-tolerant schemes for quantum computation [2], quantum information theory has earned a lasting and prominent place at the foundations of computer science. But at present this discipline seems rather isolated from most of the rest of physics. Will this change in the future? How might it change?

One view is that thinking about information theory will lead us to a deeper understanding of the foundations of quantum mechanics. This vision has been vividly expressed by John Wheeler [3]; Bill Wootters [9] and Chris Fuchs [5] have been among its particularly eloquent spokespersons. But I am not convinced in my heart that we are supposed to understand the foundations of quantum mechanics much better than we currently do. So I prefer to look in a different direction to anticipate where quantum information may have an impact on physics.

What I tend to find most exciting in science are ideas that can build bridges across the traditional boundaries between disciplines. Perhaps that is why I find quantum computation appealing — it has established an unprecedentedly deep link between the foundations of computer science and the foundations of physics. Truly great ideas in science tend to have broad consequences that can't be anticipated easily.

Now the quantum information community is sitting atop two ideas with potential for greatness: quantum computation and quantum error correction. I'd like to

suggest two directions in which quantum information theory might evolve in the future that could lead to broad and exciting consequences for other subfields of physics. These are:

### 1. Precision measurement.

Our deepening understanding of quantum information may lead to new strategies for pushing back the boundaries of quantum-limited measurements. Quantum entanglement, quantum error correction, and quantum information processing might all be exploited to improve the information-gathering capability of physics experiments.

### 2. Many-body quantum entanglement.

The most challenging and interesting problems in quantum dynamics involve understanding the behavior of strongly-coupled many-body systems — systems with many degrees of freedom that undergo large quantum fluctuations. Better ways of characterizing and classifying the features of many-particle entanglement may lead to new and more effective methods for understanding the dynamical behavior of complex quantum systems.

## II. QUANTUM INFORMATION THEORY AND PRECISION MEASUREMENT

The connections between quantum information and precision measurement are explored in a separate article [6], which I will only summarize here.

My own interest in the quantum limitations on precision measurement has been spurred in part by Caltech's heavy involvement in the LIGO project, the Laser Interferometer Gravitational-Wave Observatory [7]. LIGO is scheduled to begin collecting data in 2002, and a major upgrade is planned for two years later, which will boost the optical power in the interferometer and improve the sensitivity. In its most sensitive frequency band, the LIGO II observatory will actually be operating at the standard quantum limit (SQL) for detection of a weak classical force by monitoring a free mass. (In this case, the SQL corresponds to a force that nudges an 11 kg mass by about  $10^{-17}$  cm at a frequency of 100 Hz.)

Then within another 4 years (by 2008), another upgrade is expected, which will boost the sensitivity in the most critical frequency band beyond the SQL. Even an improvement by a factor of two can have a very significant

---

\*CALT-68-2219

<sup>†</sup>preskill@theory.caltech.edu

payoff, for a factor of two in sensitivity means a factor of 8 in event rate. But the design of the LIGO III detection system is still largely undecided — clever innovations will be needed. So Big Science will meet quantum measurement in the first decade of the new century, and ideas from quantum information theory may steer the subsequent developments in detection of gravitational waves and other weak forces.

I learned the right way to think about the quantum limits on measurement sensitivity from Hideo Mabuchi [8] — in a quantum measurement, a classical signal is conveyed over a quantum channel.<sup>1</sup> Nature sends us a message, a weak classical force, that can be regarded as a classical parameter appearing in the Hamiltonian of the apparatus (or more properly, if there is noise, a master equation). The apparatus undergoes a quantum operation  $\mathcal{S}(a)$ , and we are to extract as much information as we can about the parameter(s)  $a$  by choosing an initial preparation of the apparatus, and a POVM to read it out. Quantum information theory should be able to provide a theory of the *distinguishability of superoperators*, a measure of how much information we can extract that distinguishes one superoperator from another, given some specified resources that are available for the purpose. This distinguishability measure would characterize the inviolable limits on measurement precision that can be achieved with fixed resources.

I don't know exactly what shape this nascent theory of the distinguishability of superoperators should take, but there are already some highly suggestive hints that progress in quantum information processing can promote the development of new strategies for performing high-precision measurements.

### A. Superdense coding: improved distinguishability through entanglement

A watchword of quantum information theory is: “Entanglement is a Useful Resource.” It should not be a surprise if entanglement can extend the capabilities of the laboratory physicist.

For example, the phenomenon of superdense coding illustrates that shared entanglement can enhance classical communication between two parties [13]. The same strategy can sometimes be used to exploit entanglement to improve the distinguishability among Hamiltonians (an idea suggested by Chris Fuchs [14]). Suppose I wish to

---

<sup>1</sup>Of course, connections between quantum information theory and precision measurement have been recognized by many authors. Especially relevant is the work by Wootters [9], by Braunstein [10], and by Braunstein and Caves [11] on state distinguishability and parameter estimation, and by Braginsky and others [12] on quantum nondemolition measurement.

observe the precession of spin-1/2 objects to determine the value of an unknown magnetic field. If two spins are available, one way to estimate the value of the unknown field is to allow both spins to precess in the field independently, and then measure them separately. An alternative method is to prepare an entangled Bell pair, expose one of the two spins to the magnetic field while the other is carefully shielded from the field, and finally carry out a collective Bell measurement on the pair. It turns out that in many cases (for example when we have no *a priori* knowledge about the field direction), the entangled strategy extracts more information about the unknown field than the strategy in which uncorrelated spins are measured one at a time [6]. This separation still holds even if we allow the unentangled strategy to be *adaptive*; that is, even if the outcome of the measurement of the first spin is permitted to influence the choice of the measurement that is performed on the second spin.

### B. Grover's database search: improved distinguishability through driving

An important paradigm emerging from the recent studies of quantum algorithms is Grover's method for rapidly searching an unsorted database [15]. Farhi and Gutmann [16] observed that Grover's algorithm may be interpreted as a method for improving the distinguishability of a set of Hamiltonians by adding a controlled driving term.

In the formulation they suggested, the Hamiltonian acting in an  $N$ -dimensional Hilbert space is known to be one of the operators

$$H_x = E|x\rangle\langle x|, \quad (1)$$

where  $\{|x\rangle, x = 0, 1, \dots, N-1\}$  is an orthonormal basis. We may gain information about the value of  $x$  by preparing states, allowing them to evolve under  $H_x$  for a while, and then measuring suitable observables. But determining the value of  $x$  by this strategy requires a total time of order  $N$ . A more effective strategy is to modify the Hamiltonian by adding a controlled driving term

$$H_D = E|s\rangle\langle s|, \quad (2)$$

where  $|s\rangle = N^{-1/2} \sum_{y=0}^{N-1} |y\rangle$ , so that the full Hamiltonian becomes  $H'_x = H_x + H_D$ . If the initial state  $|s\rangle$  is prepared and allowed to evolve under  $H'_x$  for a time  $T = \pi\sqrt{N}/2E$ , then an orthogonal measurement in the  $\{|x\rangle\}$  basis will reveal the true identity of the Hamiltonian. The time required is of order  $\sqrt{N}$ ; this is Grover's quadratic speed-up.

In this Grover-Farhi-Gutmann problem, there is a sense in which an optimal measurement procedure is known: Just as the Grover iteration allows one to identify a marked state with a minimum number of queries to the oracle [17], the Grover perturbation allows us to

identify the actual Hamiltonian in the minimal elapsed time (asymptotically for large  $N$ ).

Grover’s algorithm presumes the existence of a quantum oracle that can reply to coherent queries. In an algorithmic setting, the oracle may be regarded as a quantum circuit that can be executed repeatedly. In experimental physics, the quantum oracle is Nature, whose secrets we are eager to expose. The experimenter is challenged to find the most effective (and practical!) way to query Nature and learn her Truths.

### C. Semiclassical quantum Fourier transform as adaptive phase measurement

Shor’s quantum factoring algorithm [1], which apparently achieves an exponential speed-up relative to classical algorithms, is based on the efficient quantum Fourier transform (QFT). Fourier analysis is a versatile tool in the laboratory, so we might expect the fast QFT to have important applications to physics.

One example could be the high-precision measurement of a frequency, like the energy splitting between the ground state and an excited state of an atom [6]. As Cleve *et al.* [18] have emphasized, the QFT can be viewed as a procedure for estimating an unknown phase. With a quantum computer, we could execute the quantum Fourier transform on  $n$  two-level atoms, and then read out a result by measuring the internal state of each atom. If losses are negligible, the measurement outcomes provide an estimate of the frequency to an accuracy of order  $2^{-n}$ . This procedure makes optimal use of an essential resource (the number of atoms measured), in that about one bit of information about the frequency is acquired in each binary measurement.

In fact, the complexity of the quantum information processing needed to execute this protocol is modest. In its “semiclassical” implementation proposed by Griffiths and Niu [19], the QFT is an *adaptive* procedure for phase estimation that makes use of the information collected in previous measurements to extract the best possible information from subsequent measurements. Less significant bits of the phase are measured first, and the measurement results are used to determine what single-qubit phase rotations should be applied to other qubits to extract the more significant bits more reliably. In conventional Ramsey spectroscopy, these single-qubit transformations are applied simply by prescribing the proper time interval between the Ramsey pulses.

These and other related examples give strong hints that ideas emerging from the theory of quantum information and computation are destined to profoundly influence the experimental physics techniques of the future.

## III. MANY-BODY ENTANGLEMENT AND STRONGLY-COUPLED QUANTUM PHYSICS

### A. Some signposts in Hilbert space

The most challenging and interesting problems in quantum mechanics concern many-body systems with strong quantum fluctuations. An important goal is to understand the dynamics of such systems, but it is not easy. Indeed, it is largely because strongly-coupled quantum dynamics is so difficult to understand that we want so badly to build a quantum computer [20]!

I expect that, short of building a full-blown quantum simulator, there are many possible theoretical advances that potentially could enhance our understanding of strongly-coupled systems, including advances that could emerge from the theory of quantum information. A central task of quantum information theory has been to characterize and quantify the entanglement of multipartite systems. Up until now, most attention has focused on systems divided into a small number of parts (like two<sup>2</sup>), but also of great importance are the properties of  $n$ -body entanglement in the limit of large  $n$ . Studies of these properties may give us some guidance concerning what quantum simulation problems are genuinely computationally difficult, and may suggest to experimenters what kinds of systems are most likely to exhibit qualitatively new phenomena.

Hilbert space is a big place [22], and so far we have become familiar with only a tiny part of it. In its unexplored vastness, there is sure to be exciting new physics to discover. But much of Hilbert space is bound to be very boring indeed, so we will need some clear signposts to show the way to the exotic new phenomena.

It is truism (but still profoundly true!) that More is Different [23]. So many of the collective phenomena exhibited by many-body systems (crystals, phase transitions, superconductivity, fractional quantum Hall effect, ...) would be exceedingly hard to predict from first principles. That’s good news for experimenters — marvelous things could happen in many-body systems that we have been unable to anticipate. But it is easier to find something new when theory can provide some guidance.

### B. Quantum error-correcting codes

A prototype for many-body entanglement has been developed in the past few years: the quantum error-correcting codes [24]. For example, a (nondegenerate) code that can correct any  $t$  errors in a block of  $n$  qubits has the property that no information resides in any set of  $2t$  qubits chosen from the block – the density matrix of

---

<sup>2</sup>See [21], for example.

the  $2t$  qubits is completely random. Information *can* be encoded in the block, but the encoded information has a *global* character; there is no way to access any information at all by looking at only a few qubits at a time.

For example, associated with the familiar five-qubit code [21,25] that can protect a single encoded qubit from an error afflicting any of the five qubits in the code block, there is a maximally entangled six-qubit pure state. This state has the property that if we trace over any three of the qubits, the density matrix of the remaining three is a multiple of the identity. It has been recognized only rather recently how unusual this state is [26]: there exist no  $2n$ -qubit states with  $n$  larger than three such that tracing over half of the qubits leaves the other half in a completely random state.<sup>3</sup>

Asymptotically, we don't know precisely "how entangled" an  $n$ -qubit state can be, but there are useful upper and lower bounds. For large  $n$ , the number  $s$  of qubits such that the density matrix for any  $s$  of the  $n$  is random, *must* satisfy  $s/n < 1/3$  [28]. On the other hand, states with this property are known to exist for  $s/n \leq .1893\dots$  [29]. Somewhere between  $1/3$  and  $.1893$ , there is a critical value that has not yet been pinned down. These upper and lower bounds are instructive examples of interesting results regarding multi-body entanglement that have emerged from the study of quantum error-correcting codes.

### C. Classes of entangled states

This kind of global encoding of information is actually found in some systems that can be realized in the laboratory, such as systems that exhibit the fractional quantum Hall effect [30], or certain kinds of frustrated antiferromagnets. These systems have in common that the microscopic degrees of freedom are locally "frustrated" – that is, they are unable to find a configuration that satisfactorily minimizes the local energy density. In response, the system seeks an unusual collective state that relieves the frustration, a state such that the microscopic degrees of freedom are profoundly entangled. Condensed matter physicists have found useful ways to characterize the global properties of the entanglement that results.

For example, in the case of a two-dimensional system, we may consider how the ground state degeneracy of the system behaves on a topologically nontrivial surface in the thermodynamic limit. As Wen [31] emphasized, in fractional quantum Hall systems the degeneracy increases with the genus (number of handles) of the surface as

$$\text{ground state degeneracy} \sim (A)^{\text{genus}}. \quad (3)$$

---

<sup>3</sup>But there *are* such maximally entangled states with more than six parts if each part is a higher-dimensional system rather than a qubit [27].

This dependence arises from the "winding" of entanglement around the handles of the surface, and the value of  $A$  distinguishes qualitatively different types of entangled states that must be separated from one another by phase boundaries. Just such a topological degeneracy is exploited in the ingenious quantum error-correcting codes constructed by Alexei Kitaev [32]. A closely related observation is that in a two-dimensional system with a boundary, there can be excitations confined to the boundary, and the properties of these edge excitations reflect the nature of the entanglement in the bulk system [33].

I am hopeful that quantum information theory may lead to other as yet unknown ways to characterize the entangled many-body ground states of condensed matter systems, which may suggest new types of collective phenomena. We should also advance our understanding of how the profoundly entangled systems that Nature already provides might be exploited for stable storage of quantum information.

### D. Information and renormalization group flow

The renormalization group (RG), one of the most profound ideas in science, is another topic that might be profoundly elucidated by an information-theoretic approach. Especially in the hands of Ken Wilson [34], the RG spawned one of the central unifying insights of modern physics, that of *universality* — physics at long distances can be quite insensitive to the details of physics at much shorter distances. Indeed, for the purpose of describing the long-distance physics, all of the short-distance physics can be absorbed into the values of the parameters of an *effective field theory*, where the number of parameters needed is modest if we are content with predictions to some specified accuracy.

So it is that physics is possible at all. Fortunately, it is not necessary to grasp all the subtleties of quantum gravity at the Planck scale to understand (say) the spectrum of the hydrogen atom in great detail!

The renormalization group describes how a quantum field theory "flows" as we "integrate out" short distance physics, obtaining a new theory with a smaller value of the ultraviolet momentum cutoff  $\Lambda$ . "Universal" features are associated with the "fixed" points in the space of theories where the flow is stationary. In the neighborhood of each fixed point are a finite number of independent directions in theory space along which the flow is repelled by the fixed point, the "relevant" directions of flow.

Each fixed point provides a potential description of physics in the far infrared, with the number of free ("renormalized") parameters in the description given by the number of relevant directions of flow away from the fixed point. Infrared theories with more parameters are less generic, in the sense that more "bare" parameters in the microscopic Hamiltonian of the system need to be

carefully tuned in order for the flow to avoid all relevant directions and hence carry the theory to the vicinity of the fixed point. Typically, RG flow will carry a theory from the vicinity of a less generic fixed point toward the vicinity of a more generic fixed point.

Now there is at least a heuristic sense in which information is lost as a theory flows along an RG trajectory — the infrared theory “forgets” about its ultraviolet origins. One of the most intriguing challenges at the interface of physics and information is to make this connection more concrete.<sup>4</sup> Can we quantify how much information is discarded when a theory flows from the vicinity of one fixed point to the vicinity of another?

The proposal that an effective theory forgets more and more about its microscopic origins under RG flow leads to a robust expectation. RG flow should be a *gradient* flow: it always runs downhill (toward “less information”), and never uphill (toward “more information”). Indeed, this property *does* hold for translationally invariant and relativistically invariant quantum field theories in one spatial dimension. Zamolodchikov’s *c-theorem* [36] identifies a function  $C$  of the parameters in the Hamiltonian that can be extracted from the two-point correlation function of the conserved energy-momentum tensor, and shows that  $C$  is non-increasing along an RG trajectory. At a fixed point, the quantity  $C$  coincides with the central charge  $c$  that characterizes the representation of the conformal algebra according to which the fields of the fixed-point theory transform. Last year, an extension of this result to higher even-dimensional spacetimes was reported [37] (following a suggestion by Cardy [38]).

It seems natural that the Zamolodchikov  $C$ -function should have a sharp interpretation relating it to loss of information along the flow, but none such is known (at least to me). A more precise information-theoretic interpretation of RG flow might guide the way to more general formulations of the *c*-theorem, applicable for example to theories in odd-dimensional spacetimes and to theories with less symmetry. And it might enrich our understanding of the classification of fixed-point theories and the general structure of renormalization group flow.

### E. Bulk-boundary interactions

If the information-theoretic foundations underlying the *c*-theorem continue to prove elusive, there is another related problem that might turn out to be more tractable. It is known that a one-dimensional system with a *boundary* (like a semi-infinite antiferromagnetic spin chain) can sometimes exhibit an anomalous zero-temperature entropy. The entropy has a piece proportional to the length of the chain that vanishes as  $T \rightarrow 0$ , but there

is also a length-independent contribution that is nonvanishing at zero temperature (discovered by Cardy [39] and by Affleck and Ludwig [40]). Ordinarily, we expect that zero-temperature entropy has an interpretation in terms of ground-state degeneracy, but in these systems (which have no mass gap, so that the ground-state degeneracy becomes a subtle concept in the thermodynamic limit),  $g = e^{S(T=0)}$  is not an integer; hence the interpretation of the entropy is obscure.

A fascinating feature is that the “ground-state degeneracy”  $g$  is a *universal* property — in the vicinity of an RG fixed point, its value is insensitive to the ultraviolet details (the microscopic interactions among the spins in the chain). Furthermore, there is evidence for a *g*-theorem;  $g$  has a smaller value at more generic fixed points and a larger value at less generic fixed points [40].

The *g*-theorem, like the *c*-theorem, invites an interpretation in terms of loss of information along an RG trajectory. But I am hopeful that the information-theoretic origin of the *g*-theorem may turn out to be easier to understand. Upon hearing of entropy at zero temperature, a quantum information theorist’s ears prick up — it sounds like entanglement. It is tempting to interpret the entropy as arising from entanglement of degrees of freedom isolated at the boundary of the chain with degrees of freedom that reside in the bulk. So far, I have been unable to find a precise interpretation of this sort, but I still suspect that it could be possible.

### F. Holographic universe

While on the subject of bulk-boundary interactions, I should mention the most grandiose such interaction of all. A new view of the quantum mechanics of spacetime is emerging from recent work in string theory, according to which the quantum information encoded in a spatial volume can be read completely on the surface that bounds the volume (“the holographic principle”) [41]. This too has a whiff of entanglement — for we have seen that in a profoundly entangled state the amount of information stored locally in the microscopic degrees of freedom can be far less than we would naively expect. (Think of a quantum error-correcting code, in which the encoded information may occupy a small “global” subspace of a much larger Hilbert space.) The holographic viewpoint is particularly powerful in the case of the quantum behavior of a black hole. The information that disappears behind the event horizon can be completely encoded on the horizon, and so can be transferred to the outgoing Hawking radiation [42] that is emitted as the black hole evaporates. This way, the evaporation process need not destroy any quantum information.

As the evidence supporting the holographic principle mounts [43], an unsettling question becomes more deeply puzzling: If quantum information can be encoded completely on the boundary, why does physics seem to be

---

<sup>4</sup>For an interesting recent attempt, see [35].

local? It's strange that I imagine that I can reach out and embrace you, when we are both just shadows projected on the wall. Perhaps as the tools for analyzing many-body entanglement grow more powerful, we can begin to grasp the origin of the persistent illusion that physics is founded on the locality of spacetime.<sup>5</sup>

#### IV. CONCLUSIONS

In the future, I expect quantum information to solidify its central position at the foundations of computer science, and also to erect bridges that connect with precision measurement, condensed matter physics, quantum field theory, quantum gravity, and other fields that we can only guess at today. I have identified two general areas in which I feel such connections may prove to be particularly enlightening. Progress in quantum information processing may guide the development of new ideas for improving the information-gathering capabilities of physics experiments. And a richer classification of the phases exhibited by highly entangled many-body systems may deepen our appreciation of the wealth of phenomena that can be realized by strongly-coupled quantum systems.

#### ACKNOWLEDGMENTS

My work on the applications of quantum information theory to quantum-limited measurements has been in collaboration with Andrew Childs and Joe Renes [6]. I'm very grateful to Hideo Mabuchi for stimulating my interest in that subject, and to Dave Beckman and Chris Fuchs for their helpful suggestions. I have also benefitted from discussions about precision measurement with Constantin Brif, Jon Dowling, Steven van Enk, Jeff Kimble, Alesha Kitaev, and Kip Thorne. I thank Michael Nielsen for emphasizing the relevance of quantum information in quantum critical phenomena, Ian Affleck for enlightening correspondence about conformal field theory, Anton Kapustin for a discussion about Ref. [37], Dorje Brody for informing me about Ref. [35], and Curt Callan for encouragement. Finally, I am indebted to Ike Chuang for challenging me to speculate about the future of quantum information theory. This work has been supported in part by the Department of Energy under Grant No. DE-FG03-92-ER40701, and by DARPA through the Quantum Information and Computation (QUIC) project administered by the Army Research Office under Grant No. DAAH04-96-1-0386.

---

<sup>5</sup>A different possible connection between quantum error-correcting codes and the black-hole information puzzle was suggested in [44].

- 
- [1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, p. 124 (IEEE Computer Society Press, Los Alamitos, CA, 1994), quant-ph/9508027.
  - [2] P. W. Shor, "Fault-tolerant quantum computation," *Proceedings of the 37th Annual Symposium on the Foundations of Computer Science*, p. 56 (IEEE Computer Society Press, Los Alamitos, CA, 1996), quant-ph/9605011.
  - [3] J. A. Wheeler, "Information, physics, quantum: the search for links," in *Proc. 3rd Int. Symp. Foundations of Quantum Mechanics* (Tokyo, 1989), p. 354.
  - [4] W. K. Wootters. *The Acquisition of Information from Quantum Measurements*, Ph.D. thesis, the University of Texas at Austin (1980).
  - [5] C. A. Fuchs, "The structure of quantum information," (1997), unpublished.
  - [6] A. M. Childs, J. Preskill, and J. Renes, "Quantum information and precision measurement," quant-ph/9904021 (1999).
  - [7] P. Fritschel, "The LIGO Project: Progress and Plans," *Proceedings of the Second Edoardo Amaldi Conference on Gravitational Waves* (1997).
  - [8] H. Mabuchi, "Dynamical identification of open quantum systems," *Quantum Semiclass. Opt.* **8**, 1103 (1996), quant-ph/9608020.
  - [9] W. K. Wootters, "Statistical distance and Hilbert space," *Phys. Rev. D* **23**, 357 (1981).
  - [10] S. L. Braunstein, "Quantum limits on precision measurement of phase," *Phys. Rev. Lett.* **69**, 3598 (1992)
  - [11] S. L. Braunstein and C. Caves, "Statistical distance and the geometry of quantum states," *Phys. Rev. Lett.* **72**, 3439 (1994).
  - [12] V. B. Braginsky and F. Ya. Khalili, *Quantum Measurement* (Cambridge University Press, Cambridge, 1992).
  - [13] 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).
  - [14] C. A. Fuchs, private communication (1998).
  - [15] L. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Phys. Rev. Lett.* **79**, 325 (1997), quant-ph/9706033.
  - [16] E. Farhi and S. Gutmann, "An analog analogue of a digital quantum computation," quant-ph/9612026 (1996).
  - [17] C. B. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," quant-ph/9701001 (1997); C. Zalka, "Grover's quantum searching algorithm is optimal," quant-ph/9711070 (1997).
  - [18] R. Cleve, A. Ekert, C. Macchiavello, M. Mosca, "Quantum algorithms revisited," *Proc. Roy. Soc. Lond. A* **454**, 339 (1998), quant-ph/9708016.
  - [19] R. B. Griffiths and C.-S. Niu, "Semiclassical Fourier transform for quantum computation," *Phys. Rev. Lett.*

- 76**, 3228 (1996), quant-ph/9511007.
- [20] R. P. Feynman, “Simulating physics with computers,” *Int. J. Theor. Phys.* **21**, 467 (1982).
- [21] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters, “Mixed state entanglement and quantum error correction,” *Phys. Rev. A* **54**, 3824 (1996), quant-ph/9604024.
- [22] 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*, ed. A. Mann and M. Revzen, *Ann. Israel Phys. Soc.* **12**, 226 (1996).
- [23] P. W. Anderson, “More is different,” *Science* **177**, 393 (1972).
- [24] P. W. Shor, “Scheme for reducing decoherence in quantum memory,” *Phys. Rev. A* **52**, 2493 (1995); A. M. Steane, “Error correcting codes in quantum theory,” *Phys. Rev. Lett.* **77**, 793 (1996).
- [25] R. Laflamme, C. Miquel, J. P. Paz, and W. Zurek, “Perfect quantum error correction code,” *Phys. Rev. Lett.* **77**, 198 (1996), quant-ph/9602019.
- [26] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, “Quantum error correction via codes over GF(4),” quant-ph/9608006 (1996).
- [27] R. Cleve, D. Gottesman, and H.-K. Lo, “How to share a quantum secret,” quant-ph/9901025 (1999).
- [28] E. M. Rains, “Quantum shadow enumerators,” *IEEE Trans. Inf. Theory*, quant-ph/9611001 (1996).
- [29] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, “Quantum error correction and orthogonal geometry,” *Phys. Rev. Lett.* **78**, 405 (1997), quant-ph/9605005.
- [30] M. Stone (ed.), *The Quantum Hall Effect* (World Scientific, Singapore, 1992).
- [31] X.G. Wen, “Topological order in rigid states,” *Int. J. Mod. Phys. B* **4**, 239 (1990).
- [32] A. Yu. Kitaev, “Quantum error correction with imperfect gates,” in *Quantum Communication, Computing, and Measurement (Proc. 3rd International Conference of Quantum Communication and Measurement)*, p. 181 (Plenum Press, New York, 1997); A. Yu. Kitaev, “Fault-tolerant quantum computation by anyons,” quant-ph/9707021 (1997).
- [33] X.G. Wen, “Electrodynamical properties of gapless edge excitations in the fractional quantum Hall states,” *Phys. Rev. Lett.* **64**, 2206 (1990).
- [34] K. G. Wilson and J. Kogut, “The renormalization group and the epsilon expansion,” *Phys. Rep.* **12**, 75 (1974).
- [35] D. C. Brody and A. Ritz, “On the symmetry of real-space renormalization,” *Nucl. Phys.* **B522**, 588 (1998).
- [36] A. B. Zamolodchikov, “‘Irreversibility’ of the flux of the renormalization group in a 2-D field theory,” *JETP Lett.* **43**, 730 (1986) [*Pisma Zh. Eksp. Teor. Fiz.* **43** 565 (1986)].
- [37] S. Forte, J. I. Latorre, “A proof of the irreversibility of renormalization group flows in four dimensions,” *Nucl. Phys.* **B535**, 709 (1998), hep-th/9805015.
- [38] J.L. Cardy, “Is there a c-theorem in four dimensions?,” *Phys. Lett.* **B215**, 749 (1988).
- [39] J. L. Cardy, “Boundary conditions, fusion rules, and the Verlinde formula,” *Nucl. Phys.* **B324**, 581 (1989).
- [40] I. Affleck and A. W. W. Ludwig, “Universal noninteger ‘ground-state degeneracy’ in critical quantum systems,” *Phys. Rev. Lett.* **67**, 161 (1991).
- [41] C. R. Stephens, G. ’t Hooft, B. F. Whiting, “Black hole evaporation without information loss,” *Class. Quant. Grav.* **11**, 621 (1994), gr-qc/9310006; L. Susskind, “The world as a hologram,” *J. Math. Phys.* **36**, 6377 (1995), hep-th/9409089.
- [42] S. W. Hawking, “Particle creation by black holes,” *Comm. Math. Phys.* **43**, 199 (1975).
- [43] J. Maldacena, “The large- $N$  limit of superconformal field theories and supergravity,” *Adv. Theor. Math. Phys.* **2**, 231 (1998), hep-th/9711200.
- [44] J. Preskill, “Fault-tolerant quantum computation,” in *Introduction to Quantum Computation and Information*, eds. H.-K. Lo, S. Popescu, and T. Spiller, (World Scientific, New Jersey, 1998), p. 213, quant-ph/9712048.