To balance a pencil on its tip: on the passive approach to quantum error correction

Amit Hagar

Department of History & Philosophy of Science, College of Arts & Sciences, Indiana University, Bloomington, IN

(Dated: January 10, 2011)

The passive approach to quantum error correction is analyzed within the context of the foundations of classical statistical mechanics. This allows us to formulate more precisely a skeptical conjecture on the feasibility of large-scale, fault-tolerant and computationally superior quantum computers.

Keywords: Computational Complexity; Decoherence Free Subspaces; Fluctuation Theorems; Noiseless Subsystems; Quantum Error Correction; Quantum Zeno Effect; Statistical Mechanics; Threshold Theorems

I. INTRODUCTION

Quantum computers are hypothetical quantum information processing (QIP) devices that allow one to store, manipulate, and extract information while harnessing quantum physics to solve various computational problems and do so putatively more efficiently than any known classical counterpart. Despite many proofs of concept (also known as the ‘threshold theorems’, e.g., Aharonov & Ben–Or, 1996; Knill & Laflamme, 1996; Knill et al., 1996; Knill et al., 1998), the key obstacle in realizing these powerful machines remains their scalability and susceptibility to noise: almost three decades after their conceptions, experimentalists still struggle to maintain useful quantum coherence in QIP devices with more than a pair of qubits (e.g., Blatt & Wineland, 2008). This slow progress has prompted debates on the feasibility of large-scale, fault-tolerant and computationally superior quantum computers.

The passive approach to quantum error correction bifurcated early on from the main path taken by quantum computer scientists (Barenco et al., 1997; Zanardi & Rasetti, 1997; Lidar et al., 1998; Viola et al., 1999). The idea behind it is to look for those regions in the device’s state space which are thermodynamically abnormal, i.e., those regions in the device’s state space which resist thermalization regardless of external noise.

This paper is intended as a further contribution to the debate on the feasibility of large-scale, fault-tolerant and computationally superior quantum computers. Relying again on analogies from the foundations of classical SM, it suggests a skeptical conjecture and frames it in the passive, error avoidance, context. To be clear, while I do hint at various routes in which such a conjecture could be proven, in doing so I do not pretend to present a ‘no-go’ argument nor a definitive skeptical attack; my sole intention is to make the debate more precise. Moreover, even if this skeptical conjecture turned out to be true, this would not render QIP devices useless; one might still use them to outperform existing classical computers for certain designated tasks that require only few qubits. It would mean, however, that the aforementioned threshold theorems that support the feasibility of an arbitrarily scalable computationally superior quantum computation were misleading.

The paper is structured as follows. In section 2 I sketch the passive approach to quantum error correction. Section 3 presents the main background for the statistical mechanical analogy that drives my argument, namely, Boltzmann’s combinatorial approach to the problem of the thermodynamic arrow in time. In section 4 I present the skeptical conjecture I believe can (and should) be made precise using this analogy, and give several hints how to pursue a possible proof thereof. Limited conclusions are given in Section 5.

II. THE PASSIVE APPROACH TO QUANTUM ERROR CORRECTION

The passive approach to quantum error correction bifurcated early on from the main path taken by quantum computer scientists (Barenco et al., 1997; Zanardi & Rasetti, 1997; Lidar et al., 1998; Viola et al., 1999). The idea behind it is to look for those regions in the system’s state space which are unaffected by the interaction of the system with its environment. Given the robustness of these regions, if one were able to encode information into them, this information would remain intact during the system’s evolution, and one could then manipulate it, presumably using fault-tolerant gates and other tech-
niques from the arsenal of active error correction.

Let us give a classical example to this idea using one of the simplest error avoiding codes. Assume we have an error process that with some probability flips all bits in a group, and otherwise does nothing. In this case we can encode a classical bit as

$$0 \rightarrow 00, \quad 1 \rightarrow 01.$$  

The error process will change the encoded states to

$$00 \rightarrow 11, \quad 01 \rightarrow 10.$$  

Note that the parity of the two bits is conserved no matter whether the error has acted or not. So when we decode, we will associate 00 and 11 with the encoded 0 bit and 01 and 10 with the encoded 1. Note also that we will be able to decode correctly no matter how high the rate of error is! The error does not touch the invariant, parity ‘space’, into which we encode. That means that our encoded information has managed to completely avoid the error.

In quantum systems, invariant quantities are associated with the presence of symmetries, that is, with operators that commute with all possible errors. For one of the most common collective decoherence processes, the noise operators on $n$ qubits are given by $S_\alpha = \sum_{i=1}^{n} \sigma_i^{(2)}$, where $\sigma_i^{(2)}$ is a Pauli matrix ($\alpha = \{x, y, z\}$) on the $i$th qubit (see appendix). Intuitively this means that the possible unitary errors are $\exp(itS_\alpha)$. An error–free subspace exists when

$$S_\alpha|\text{codeword}\rangle = c_\alpha|\text{codeword}\rangle,$$

or, in other words, when the code space is a simultaneous eigenspace of each $S_\alpha$ with eigenvalue $c_\alpha$. If this is the case, each unitary noise operator only introduces an unobservable phase $\exp(itc_\alpha)$ on the code space. In a trivial two–qubit example (see appendix), where the state of qubit 1 is stored in the state of qubit 2 without being affected by the errors, operators acting only on the second qubit commute with the error operators. In particular, if $E$ is any one of the errors, then $E\sigma_\alpha^{(2)} = \sigma_\alpha^{(2)}E$, for $\alpha = x, y, z$. It follows that the expectations of $\sigma_\alpha^{(2)}$ are conserved. That is, if $\rho$ is the initial state (density matrix) of the two physical qubits and $\rho'$ is the state after the errors acted, then $tr\sigma_\alpha^{(2)}\rho' = tr\sigma_\alpha^{(2)}\rho$. Because the state of qubit 2 is completely characterized by these expectations, it follows immediately that it is unaffected by the noise.

A less trivial example is the encoding of 4 qubits (Kempe 2005, p. 15):

$$|0\rangle_{\text{code}} = |s\rangle \otimes |s\rangle,$$

$$|1\rangle_{\text{code}} = \frac{1}{\sqrt{2}}\left(|t_+\rangle \otimes |t_-\rangle - |t_0\rangle \otimes |t_0\rangle + |t_-\rangle \otimes |t_+\rangle\right),$$

where $|s\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$ and $|t_{-0,+}\rangle = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{\sqrt{2}}$. It is easy to see that $S_\alpha|0\rangle = S_\alpha|1\rangle = 0$ for $\alpha = \{x, y, z\}$ (i.e. that the coefficients $c_\alpha = 0$). This means that both code states are invariant under collective noise. If we encode our information into the subspace spanned by $|0\rangle_{\text{code}}$ and $|1\rangle_{\text{code}}$, it will completely avoid the errors; the information resides in a ‘quiet’ part of the system’s space, dubbed as the decoherence–free subspace.

When do these ‘quiet’ subspaces exist and how can they be constructed? The trivial two–qubit example suggests a general strategy for finding a noiseless subspace: first determine the commutant of the errors, which is the set of operators that commute with all errors. Then find a subset of the commutant that is algebraically equivalent to the operators characterizing a qubit. The equivalence can be formulated as a one–to–one map from qubit operators to operators in the commutant. For the range of $f$ to be algebraically equivalent, $f$ must be linear and satisfy $f(A^{(1)}) = f(A)^{(1)}$ and $f(AB) = f(A)f(B)$. Once such an equivalence is found, a fundamental theorem from the representation theory of finite dimensional operator algebras implies that a subsystem identification for a noiseless qubit exists (Knill et al., 2000).

A noiseless subspace is thus perfect for maintaining quantum information. Yet one may argue that operations such as manipulating this information, or even storing it initially, require access to that subspace, hence disturb it. In order to eliminate such inevitable disturbances, the general strategy is to keep the information stored in the QIP device in its ‘quiet’ subspace using dynamical methods. The idea here is a generalization of the famous ‘quantum Zeno effect’ (Misra & Sudarshan 1977): one aims to keep the system in a subspace by repeatedly projecting the system into it. This projection has a nonzero failure probability so that the cumulative probability of repeated successful projection may be expected to fall with the number of projections. The quantum Zeno effect provides a means of maintaining the cumulative probability of successful projections arbitrarily close to unity. The basic principle is illustrated in the following simplified example (Barenco et al., 1997, 1543): consider a quantum system initially in state $|0\rangle$ which rotates into $|1\rangle$ with angular frequency $\omega$. The state at time $t$ (in the absence of any projections) is $\cos \omega t|0\rangle + \sin \omega t|1\rangle$. If we project this state into the subspace spanned by $|0\rangle$, then the probability of subsequent projection is $\cos^2 \omega t$. If we project repeatedly $n$ times between $t = 0$ and $t = 1$, i.e., at time intervals $\delta t = 1/n$, then the probability that all projections will be successful is

$$\left(\cos^2 \frac{\omega}{n}\right)^n \approx \left(1 - \frac{\omega^2}{n^2}\right)^n \to 1 \quad \text{as} \quad n \to \infty$$

Thus if the projections are performed with sufficient frequency then the state may be confined to the decoherence–free subspace with arbitrarily high probability. In quantum mechanics, projection operations correspond to measurements on the system, and so the above may be loosely phrased as “a frequently observed
state never evolves” or “a watched pot never boils”. A similar analysis holds for any unitary evolution of a state initially lying in the subspace.

In recent years it has been shown (e.g., Viola et al., 2000) that a variety of techniques in quantum control theory could be harnessed to keep the quantum information ‘at bay’, i.e., prevent it from straying outside the boundaries of the decoherence–free subspace. The open question, of course, is the complexity cost of these techniques, i.e., how do the resources they require scale with the size of the system, and is it here, or so I shall argue, where a skeptical conjecture on the feasibility of large scale, fault–tolerant and computationaly superior quantum computers can be formulated and be made precise.

In order to motivate this conjecture, let’s make a short detour into the foundations of classical SM.

III. LESSONS FROM THE FOUNDATIONS OF CLASSICAL STATISTICAL MECHANICS

Classical SM is the branch of theoretical physics that aims to account for the thermal behavior of macroscopic bodies in terms of a classical mechanical model of their microscopic constituents with the help of probabilistic assumptions. A recent discussion on active error correction (Hagar, 2009) has pointed out several analogies that exist between the foundations of this branch and the debate on the feasibility of large scale, fault–tolerant and computationaly superior quantum computers. In this section I too shall rely on the foundations of classical SM again, and in particular on the combinatorial approach of Boltzmann, for the purpose of motivating the skeptical conjecture in the context of the passive approach to quantum error avoidance.

In his response to criticism mounted against the (in)famous dynamical ‘derivation’ of the second law of thermodynamics (also known as the $H$–theorem), and in particular to Loschmidt’s reversibility objection, Boltzmann shifted to what is known today as the probabilistic, or combinatorial, approach (Uffink 2006, pp. 55–64; Brown et al., 2009, section 8). In this approach, instead of trying to underpin the thermodynamic arrow in time in the system’s dynamics, as he did with his $H$–theorem, Boltzmann attempted to re-state the empirical fact encapsulated in the second law of thermodynamics by introducing several assumptions with which he described the approach to equilibrium as a tendency for the system to evolve towards ever more probable macrostates, until, in equilibrium, it has reached the most probable state.  

The details of Boltzmann’s combinatorial approach as they are spelled out in his papers and summarized succinctly in Uffink (2006) need not concern us, and it is certainly not my intention to enter into a debate about its relative plausibility viz. other approaches to the foundations of classical SM. The important lesson I am interested to highlight instead is that with the help of several assumptions — e.g., a distinction between macro– and micro–states, the equiprobability of each microstate in a given energy shell, a specific ‘carving’ of $\mu$ space into finite cells, or partitions, the limited applicability of these assumptions to ideal gases — Boltzmann succeeds in attributing probabilities to volumes of phase space, and consequently re–describes thermalization in statistical mechanical terms.

In Boltzmann’s combinatorial approach the tendency to evolve from improbable to more probable states is presented as a fact of experience rather than the consequence of any theorem: abnormal thermal behavior (e.g., fluctuations out of equilibrium) is quite possible and consistent with the dynamical laws, but also highly improbable. In other words, in Boltzmann’s combinatorial approach abnormal thermal behavior is deemed rare, where ‘rare’ is judged relative to the standard Lebesgue measure.

Yet as Uffink (2006, p. 60) notes, whatever Boltzmann had in mind as a complete solution to the puzzle of the thermodynamic arrow in time, his combinatorial approach falls short of producing it: clearly, questions about any dynamical evolution (thermodynamically abnormal or otherwise) must be answered with appeal to the system’s initial state and Hamiltonian; arguments from measure theory alone are thus insufficient.

Among the efforts to complete Boltzmann’s attempt, perhaps the most well–known is the one supplied by the Ehrenfests, who suggest that Boltzmann somehow relied on the ergodic hypothesis in his reply to Loschmidt. But as Uffink (2006, p. 61) reminds us, the same ergodic hypothesis would imply that the system cannot stay inside the equilibrium state forever and thus there would necessarily be fluctuations in and out of equilibrium. Consequently, one would have to state that the tendency to evolve from improbable to probable states is itself a probabilistic affair; something that holds true for most of the initial states, or for most of the time, or as some or other form of average behavior.

The Ehrenfests failed to supply such a statistical extension of Boltzmann’s $H$–theorem. A famous landmark interpretations of Boltzmann’s shift see Uffink (2006, pp. 59–64).

1 On this issue there already exists a vast literature. See Frigg (2008) for a comprehensive list.

2 Clearly, Boltzmann’s combinatorial approach only makes sense with finite partitioning of $\mu$ space.

3 If the ergodic hypothesis holds, a state will spend time in the various regions of the energy shell in phase space in proportion to their volume.
towards that end was Lanford’s (1981) theorem, but more recently a group of beautiful mathematical results, known as the fluctuation theorems (Evans et al., 1993), have brought us as close as one can get to the fulfillment of Boltzmann’s combinatorial program. These results give an analytic expression for the probability, in a nonequilibrium system of finite size observed for a finite time, of a thermodynamic abnormal behavior in the reverse direction to that required by the second law of thermodynamics.

More precisely, for a dissipation function that represents a generalized entropy production, and is defined as:

$$\Omega_t(\Gamma) = \ln \left( \frac{f(\Gamma, 0)}{f(\Gamma(t), 0)} \right) + \int_0^t ds \frac{dQ(s)}{K_B T_{res}}$$

where $f(\Gamma, 0)$ is the initial phase space distribution function, $K_B$ is Boltzmann’s constant, and $dQ/dt$ is the rate of heat gained or lost per unit time by the system from a thermostat, the theorems relate the probabilities of observing time averaged values of $\Omega_t$, for a period of time, $t$, equal to an arbitrary value $A$, relative to $-A$:

$$\frac{Pr(\Omega_t = A)}{Pr(\Omega_t = -A)} = e^{A t}$$

This ratio is exponential in the length of the averaging time $t$, and the number of degrees of freedom in the system.

The result is exact for classical systems and quantum analogues are known. It confirms that for large systems, or for systems observed for long times, the second law is likely to be satisfied with overwhelming probability, systems, or for systems observed for long times, the second law is likely to be satisfied with overwhelming (exponential) likelihood: positive entropy production is overwhelmingly more probable than a negative one. Note that this also implies that as physical devices are made smaller and smaller the probability that they will run thermodynamically in reverse to what one would expect, increases exponentially with decreasing system size and observation time.

It is tempting to apply the combinatorial approach, and in particular the lesson of the fluctuation theorems to the domain of (reversible) quantum computing: the decoherence-free subspace is regarded as ‘an island of stability’ in which reversible (unitary) dynamics can go on without disturbance, resisting thermalization. In this sense, this ‘island’ harbors abnormal thermodynamic evolution, and it is natural to expect its relative size to decrease as the system becomes macroscopic. Using this analogy one might put forward the following skeptical conjecture:

$$C_0 \text{ Decoherence-free subspaces supporting quantum states that allow computational superiority become exponentially rare as the system’s size increase.}$$

But this is all too quick, for the combinatorial approach is still plagued with two persistent problems.

First, while the fluctuation theorems allow one to describe abnormal thermodynamic behavior as rare (mind you, in complete agreement with our experience), one should still specify ‘rare’ according to what measure, and subsequently justify such a choice of measure. Let’s call this problem the measure problem.

Second, and more importantly, one must also provide a link from the alleged scarcity of this much-sought-after behavior to the difficulty in observing or controlling it: on the uniform measure in phase space, for example, the vast majority of states are equilibrium states. A steam engine requires a heat source and sink of different temperatures. One could point out that states that have such temperature differentials are rare, according to this measure, but this says nothing about the feasibility of constructing a steam engine. Similarly, if we take the Haar measure, then, for a large environment, by far the vast majority of state–environment states are ones in which the system is highly entangled with its environment. Nevertheless, we believe that we can readily prepare systems in states that are pure, or close to pure.

The difficulty in providing such a link between the abstract representation of states of a physical system and the creation or manipulation of such states by the scientist signifies the limitations of the applicability of the statistical mechanical formalism to the observer. That such a link is missing from the foundations of classical SM should be regarded as one of the key problems.

---

6 Lanford’s theorem cannot be regarded as the final step in the development of the combinatorial approach since it holds only for a ridiculously short time and only in the highly unphysical Boltzmann–Grad limit of a rarified hard–sphere gas.

7 For a comprehensive review see Evans & Searles (2002).

8 The thermostat is viewed as being much larger than the system of interest and can therefore be regarded as being in thermodynamic equilibrium at a temperature $T_{res}$.

9 Recall that entropy production is extensive.

10 It should be emphasized that this theorems ‘derive’ macroscopic asymmetry from microscopic symmetry only by sneaking in an asymmetric assumption (as Boltzmann did in his $H$–theorem). Contrary to Boltzmann’s early slumber, however, the authors of this theorem are very explicit about this. See, e.g., Evans & Searles (2002, p. 1580). Also, these results are given relative to the SRB measure which is an extension of the micro–canonical measure to systems far from equilibrium. As such they fall prey to the well known problem of the justification of measure that plagues the foundations of classical SM, and is discussed below.

---

11 Two such combinatorial arguments that recently appeared in the literature are Pitowsky (2004) who, assuming a uniform measure on all possible experiments, proves that the norm of a certain entanglement witness is bounded in such a way that the probability of observing such a witness decreases exponentially with the size of a quantum system, and Gross et al. (2008), who argue that most (where ‘most’ is interpreted again relative to a specific measure) many–body entangled quantum states are useless for computational speed–up.
in that field, yet so far it has been rarely mentioned in the literature. Because of its conceptual similarity to a well-known problem in quantum theory, and for lack of a better name, I dub it here as the SM measurement problem.

Within the foundations of classical SM these two problems are still open. With respect to the first, I have no pretension to solve it here. Let me just mention that attempts to justify the choice of measure that rely on (classical) dynamical considerations are, on final account, plainly circular, stated as they are as valid for almost all cases, where the term “almost all” is defined again by an appeal to the very measure one would like to justify in the first place. Given this circularity, one may as well abandon the attempts to find such an a priori justification, and instead admit that the relation between probability in classical SM and the standard Lebesgue measure is purely an empirical matter. What I would like to suggest here instead is a solution to the second problem that not only makes the first less urgent, but also allows one to draw the analogy between the combinatorial approach to the foundations of SM and the debate on the feasibility of large scale, fault-tolerant and computationally superior quantum computers.

IV. TO BALANCE A PENCIL ON ITS TIP

Clearly, \(C_0\) is still open to objections on the basis of the two problems mentioned above, i.e., the measure problem and the SM measurement problem: it doesn’t specify the measure relative to which the decoherence-free-subspaces are deemed rare, and it doesn’t tell us anything about the computational complexity resources we need to invest in order to create them. In what follows I propose the following refinement that will allow us to replace statements about ‘rarity’ (with respect to a given measure) with statements about computational complexity. In doing so I believe one could sidestep the measure problem — dropping altogether the term ‘rare’ — and at the same time provide a link between the ‘size’ of the decoherence-free-subspace and the difficulty in preparing it.

First we need to address the notion of a ‘creation of a state’. Recall that while in classical SM a state of a physical system is defined as a probability distribution on phase space, in quantum mechanics physical states are defined as subspaces in the Hilbert space. Combined with the observation that a quantum computation is nothing more than the standard Schrödinger evolution in the computational basis from the state \(\Psi_0 = |0\rangle_1|0\rangle_2|0\rangle_3 \ldots |0\rangle_L\) to the desired output state, this conceptual difference prompts one to replace the statistical mechanical probabilistic notions with a new operational, information-theoretic, notion of ‘hardness’, explicating the latter in terms of computational complexity resources. Since the basic building block in this context is the number of computational steps, given by the number of 1–2 qubits gates that are required to generate an arbitrary state from \(\Psi_0\), the key question is how does this number scale with the size of the input (the number of qubits \(L\)).

Following the familiar definitions from computational complexity theory, we can call states whose generation requires only polynomial resources easy, and states whose generation requires exponential resources hard.

In parenthesis, it is important to be reminded that not every easy state would serve for computationally superior quantum computation. To achieve the latter we need specific entangled states that can make the probability of retrieving the result of the computation better than mere guessing (Pitowsky, 2002; Hagar & Korolev, 2007).

The best example we have today for such a state is:

\[
\frac{1}{\sqrt{2^L}} \sum_{c=0}^{2^L-1} e^{i \frac{2\pi ac}{2^L}} |c_{L-1}\rangle |c_{L-2}\rangle \ldots |c_0\rangle
\]

(4)

where \(L\) is a natural number and \(0 \leq a \leq 2^L - 1\). This superposition is the one that allows Shor’s algorithm to factor numbers into primes more efficiently than any known classical counterpart. It is a sum, with equal weights, over all possible 0, 1 states of a given length, and in its form it is similar to many such superpositions of equi-weighted sums. What makes all the difference here, however, are the phase factors \(e^{i \frac{2\pi ac}{2^L}}\) (Pitowsky 2002, p. S175).

The crucial point here is that while in the case of Shor’s algorithm the above state (4) can be generated with a number of 1–2 qubit gates polynomial in the input size \(L\) (at least in the network model of quantum computation, where arbitrary entangled states can generated from the input state \(\Psi_0\)), there is no general way of doing so in a number of computational steps (i.e., 1–2 qubit gates) which is bounded by a polynomial in \(L\).

So far we have managed to quantify how hard it is to create a certain quantum state in an ideal situation. Next we need to consider the non-ideal situation, where noise is allowed. In such a case, the theory of quantum error avoidance tells us that if the quantum state resides in its decoherence-free-subspace, it will remain intact throughout the dynamical evolution. Thus we need a way to quantify again how hard it is to maintain a computationally superior easy state inside the decoherence-free-subspace.

To this end we may return to the aforementioned method of the quantum Zeno effect that allows one to repeatedly project the quantum state back to the noiseless subspace. Recall that for a given input size, this method
succeeds in stabilizing the state, increasing the probability of the successful projections with the frequency of the projections. Now what happens if we keep the success probability (or the projection frequency) fixed but increase the input size? How does the projection frequency (or the success probability) scale in this case?

Since there exists a trade–off between the frequency of the projection that keeps a noise–resilient state in the appropriate decoherence–free subspace and the noise–level (or fault–tolerance) one aims for, to achieve better fault–tolerance one must increase the projection frequency. Consequently, if one succeeded in demonstrating exponential scaling of this frequency with the input size for a computationally superior state, it would be tantamount to demonstrating that as the dimension of the system increases, the noise–resilient subspace becomes exponentially hard to maintain. More precisely, one needs to show that for a fixed success probability, the projection frequency increases exponentially with the size of the input (or, inversely, for a fixed projection frequency, the success probability decreases exponentially). Such a proof would also entail that the unfavorable scaling of these resources offsets the alleged computational superiority that the specific state may allow in an ideal situation without the noise.

Another possible way to quantify how hard it is to create a decoherence–free-subspace stems from the algebraic formulation of the noiseless subsystem definition. This formulation allows one, under certain conditions, to reduce the problem of finding whether certain a subsystem is noise–resilient to other linear algebra problems. Progress in this context would amount to reducing the problem of finding a decoherence–free subspace to a computational problem whose complexity is known.14

What I suggest, thus, is an analogy between the combinatorial approach and quantum error avoidance that would (1) replace statements about rarity with a complexity–theoretic notion of hardness, (2) provide an operational meaning to the ‘size’ of the decoherence–free subspace, and (3) allow us to interpret this ‘size’ in terms of the resources required to keep the computationally superior state therein.

Using such an operational meaning, one can offer a slightly modified skeptical conjecture:

\[ C_1 \text{ The physical computational complexity of keeping a computationally superior quantum state in its noise–resilient (decoherence–free) subspace increases exponentially with the size of the input and offsets the putative computational superiority such a state might afford.} \]

The advantage of \( C_1 \) over \( C_0 \) is clear, but one may still object that, lacking a full–fledged theory of physical computational complexity, the suggested link between computational complexity resources and the putative difficulty in maintaining a computationally superior easy quantum state inside its noiseless subspace is not exhaustive. In other words, since there seems to be no way to uniquely formalize experimental procedures or physical interactions into quantum unitary evolutions and classify them further into computational complexity classes, the map, if there is such, between the former and the latter is clearly not bijective, hence \( C_1 \) lacks rigor, and as such is no better than \( C_0 \).

In response, let me just say that while a complete theory of physical computational complexity is indeed lacking, we can still formalize some dynamical evolutions and physical interactions in the language of quantum theory and classify these further into different complexity classes. For example, a 2–body, nearest neighbor interaction is known to be easy (in the computational complexity sense) while some many–body interactions that cannot be broken efficiently into the former are known to be hard (Wolf, 2008 and references therein). Acknowledging as I am that the field of physical computational complexity is still in its infancy, my only aim here is to initiate a line of thought, whose final goal would be a new computational complexity outlook on physics which would hopefully yield a better understanding of the relationship between the two disciplines. In this sense, a conjecture such as \( C_1 \) provokes one to study particular examples, using them a starting point for a dialectic between theoreticians and experimentalists, wherein the former present the latter with the challenge of creating increasingly complex quantum states.

Faced with this conjecture, theoreticians and experimentalists would have to re–examine known quantum systems with a new goal in mind, namely, that of quantifying the complexity resources of their respective states. Once such evidence would accumulate, and in order to lend support to \( C_1 \), quantum computing skeptics could look for a trade–off between those quantum states that can be prepared efficiently in the presence of noise (but have no computational advantage) and those that cannot (but do have such an advantage).15 Only then could the question of the feasibility of large–scale, fault–tolerant and computationally superior quantum computers be said to be well–posed.

\[ C_1 \text{ The projection frequency is ultimately related to energy (Lloyd, 2005; Somma et al., 2006).} \]

\[ 13 \text{ The projection frequency is ultimately related to energy (Lloyd, 2000; Gea–Banacloche, 2002) and heat production (Levitin & Toffoli, 2007).} \]

\[ 14 \text{ See, e.g., Knill (2006, p. 16) where the problem of deciding whether a subsystem is noise–resilient with respect to initialization procedures is shown to be polynomially equivalent to the problem of finding a matrix with orthonormal columns in a linear space of matrices. The complexity class of the latter is still unknown.} \]

\[ 15 \text{ This trade–off, if established, may also shed light on the puzzling question of why many quantum macroscopic many–body phenomena nevertheless do admit classical (efficient) simulations (Somma, 2005; Somma et al., 2006).} \]
V. CONCLUDING REMARKS

This paper was intended to demonstrate how the debate on the feasibility of large-scale, fault-tolerant and computationally superior quantum computers could be made more precise by taking into consideration some lessons from the foundations of classical SM. Ignoring these lessons, many quantum information scientists believe that the failure to realize a large-scale QIP device would indicate new physics:

If it is possible to continue scaling up such devices to a large size, the issue of the absence of cat states becomes more pressing ... If generating such states is successful, then the existence of, in essence, Schrödinger’s cats will have been shown. Such states are, however, more sensitive to the effects of phase decoherence, but this seems to be a technical, not a fundamental, problem. Therefore, if it becomes impossible to make such states or to build a large-scale quantum computer for non-technical reasons, this failure might indicate some new physics (Blatt & Wineland 2008, 1014).

C1, however, offers a different outlook, and if true, would prove both parties in the current debate wrong: contra the pessimists, large-scale, fault-tolerant and computationally superior quantum computers would be deemed physically possible, in the sense that they are consistent with the laws of physics, in particular with the laws of quantum theory and statistical mechanics, yet, contra the optimists, for the very same reason one rarely encounters abnormal thermodynamic processes in the macroscopic regime, large-scale quantum computers would be rendered impossible in practice: since preparation and manipulation of those states that can allow computationally superior and fault-tolerant quantum computation is a computationally complex task itself, QIP devices could not be scaled arbitrarily; as their size increased, they would lose their putative computational power and become no more efficient than their classical counterparts.

The possible failure of scaling up QIP devices need not render them useless. The traditional notion of efficiency (based on the distinction between polynomial and exponential growth) is an asymptotic notion referring to computations on unboundedly large inputs, and thus may not be appropriate in assessing the feasibility of particular computations in practice. For example, with more than 40 noiseless qubits a QIP device would presumably allow simulations of quantum systems beyond what is possible with classical physics. FACTORIZATION might require much more resources, but if a quantum computer could factorize a 1000-digit integer in a reasonable time it may still exceed the abilities of any classical computer for the foreseeable future albeit that the factorization of 2000-digit integers might be infeasible on any computer, quantum or classical.

This means that one should be careful when comparing quantum computation to classical computation. Conjectures such as C1 are concerned with limits, and not with arbitrary cut-offs that are contingent on human interests or commercial targets. Therefore, even if C1 turned out to be true, there might be some computational tasks for which a QIP device with a small number of noiseless qubits would still outperform a classical counterpart of a similar (or of any) size. No matter how outstanding, however, such a performance would still fall short of realizing the unqualified hope, shared by many quantum information scientists, for unlimited resilient quantum computation.

In closing, a final word of caution: so far, the number of noiseless qubits we have managed to produce in the lab is 2 (Viola et al. 2001). This tremendous achievement is clearly consistent with any statement whatsoever one could make today on the feasibility of large-scale, fault-tolerant and computationally superior QIP devices.

VI. APPENDIX

A quantum version of the classical two bit example (where the invariant, conserved, quantity under the total evolution of the system and the errors was the parity) consists of two physical qubits, where the errors randomly apply the identity or one of the Pauli operators to the first qubit. The Pauli operators are defined by

\[ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \]

(5)

Explicitly, the errors have the effect

\[ |\psi\rangle_{12} \rightarrow \begin{cases} I|\psi\rangle_{12} & \text{Probability .25} \\ \sigma_x^{(1)}|\psi\rangle_{12} & \text{Probability .25} \\ \sigma_y^{(1)}|\psi\rangle_{12} & \text{Probability .25} \\ \sigma_z^{(1)}|\psi\rangle_{12} & \text{Probability .25} \end{cases} \]

(6)

where the parenthesized superscript (1) specifies the qubit that an operator acts on. This error model is called “completely depolarizing” errors on qubit 1. Obviously, a one-qubit state can be stored in the second physical qubit without being affected by the errors. An encoding operation that implements this observation is

\[ |\psi\rangle \rightarrow |0\rangle_1|\psi\rangle_2, \]

(7)

which realizes an ideal qubit as a two-dimensional subspace of the physical qubits. This subspace is the “quantum code” for this encoding. To decode one can discard physical qubit 1 and return qubit 2, which is considered to be a natural subsystem of the physical system. In this case, the identification of syndrome and information-carrying subsystems is an obvious one. This example is taken from Knill et al. (2002), where the interested reader may find a lucid and accessible introduction to the idea of noiseless subsystem.
References


