On the (Im)possibility of Scalable Quantum Computing

Andrew Knight
aknight@alum.mit.edu
(Dated: November 7, 2021)

The potential for scalable quantum computing depends on the viability of fault tolerance and quantum error correction, by which the entropy of environmental noise is removed during a quantum computation to maintain the physical reversibility of the computer's logical qubits. However, the theory underlying quantum error correction applies a linguistic double standard to the words "noise" and "measurement" by treating environmental interactions during a quantum computation as inherently reversible, and environmental interactions at the end of a quantum computation as irreversible measurements. Specifically, quantum error correction theory models noise as interactions that are uncorrelated or that result in correlations that decay in space and/or time, thus embedding no permanent information to the environment. I challenge this assumption both on logical grounds and by discussing a hypothetical quantum computer based on "position qubits." The technological difficulties of producing a useful scalable position-qubit quantum computer parallel the overwhelming difficulties in performing a double-slit interference experiment on an object comprising a million to a billion fermions.

I. INTRODUCTION

Richard Feynman [17] famously predicted the use of a quantum computer in 1982 to simulate certain models more efficiently than a classical computer. In 1994, Peter Shor [18] proposed a quantum algorithm for factorizing integers that, if successfully implemented, would threaten encryption schemes based on prime factorization. Since then, theoretical and experimental research has forged ahead with exponential growth, funded heavily by government, university, and private equity funds.

In 2019, researchers at Google [5] claimed they had achieved "quantum supremacy" by performing a calculation in 200 seconds on a 53-qubit device that would have taken "approximately 10,000 years" on a classical supercomputer. While this claim has been disputed [25], the problem solved was not a particularly useful one and the potential applications of such a small computer are severely limited. There is optimism within the field that quantum computers can be adequately scaled upward both to achieve an indisputable quantum supremacy and – more importantly – an economically and technologically viable computer capable of solving meaningful real-world problems using exponentially fewer resources than a comparable classical computer would require.

The potential scalability of quantum computing depends on a variety of interrelated technological problems, including but not limited to:

- Creating and adequately connecting a large number of qubits. Qubits themselves can be physically instantiated in many ways, but all suffer from a variety of challenges, such as cost, size, cooling requirements, and so forth.
- Initializing qubits to desired superposition states with sufficient precision.
- Maintaining qubits in their superposition states throughout computation time with high fidelity.
- Applying one-qubit gates with high fidelity.
- Entangling qubits by applying two-qubit gates with high fidelity.
- Adequately entangling sufficiently many logical qubits with high fidelity to do something useful.

If these problems cannot all be solved, then scalable quantum computing is simply not possible. Are these merely technical problems or is there a fundamental physical limitation to the scalability of quantum computers?

While each of these problems may individually be addressed with improving technology, all are subject to the common mechanism of decoherence by environmental noise. If quantum computing is to be usefully scalable, irreversible decoherence – i.e., the kind that results in premature "measurement" of a computer's quantum state – must be prevented. In this paper I will explore the extent to which the words "noise" and "measurement" are treated by the quantum computing community with double standards, and whether this treatment is inherently fatal to the prospects for scalable quantum computing.

II. THEORY OF QUANTUM COMPUTING

A. How a Quantum Computer May Outperform a Classical Computere

A qubit is a quantum object having a state Ψ that is a superposition over binary measurement outcomes, such as $\Psi = a|0\rangle + b|1\rangle$, where a and b are complex amplitudes. A quantum computer takes advantage of entanglement between N qubits to mathematically span a 2^N-dimensional Hilbert space, allowing certain algorithms to be performed in polynomial time (or resources) that would require exponential time (or resources) in a classical computer. Because of various technical difficulties, a real quantum computer explores significantly fewer than 2^N dimensions [25].

The following example will demonstrate how a quantum computer may, at least in theory, outperform a classical computer, with the specific application of using Shor's Algorithm [18] to factor the number 15. It should be pointed out that Shor's Algorithm has never been implemented on a quantum computer. For example, Ref. [6] shows that a K-bit number can be factored by Shor's Algorithm in time K^3 with a computer acting on $5K + 1$ logical[1] qubits with $72K^3$ elementary quantum gates, a task that has never been performed for even the smallest of composite numbers. Instead, the authors describe a proof-of-principle "special purpose algorithm that could 'factor 15' with 6 qubits and only 38 pulses." However, this shortcut algorithm is useless for numbers other than 15 as it depends for its implementation on already knowing the factors.

Using the above estimates, factorizing the number 15 (which is 4 bits) requires a minimum of 21 logical qubits subjected to around 4600 gates, each of which is a member of a universal quantum gate set. Ideally, the initial state Ψ_0 of those 21 qubits is described by a 2^{21}-dimension vector in which all amplitudes are 0 except for one – specifically, the amplitude corresponding to $|111100000000000000000\rangle$, which should be 1:

$$\begin{aligned}\Psi_0 = 0\,&|000000000000000000000\rangle \\ +\, 0\,&|000000000000000000001\rangle \\ +\, 0\,&|000000000000000000010\rangle \\ +\, 0\,&|000000000000000000011\rangle + ... \\ +\, 1\,&|111100000000000000000\rangle + ... \\ +\, 0\,&|111111111111111111101\rangle \\ +\, 0\,&|111111111111111111110\rangle \\ +\, 0\,&|111111111111111111111\rangle \end{aligned} \quad (1)$$

This state is one in which the qubits are completely unentangled, the states of the first four qubits are $|1\rangle$, and the states of the remaining qubits are $|0\rangle$. To then implement Shor's Algorithm, which is mathematically just a reversible basis shift of the original vector, the qubits are acted on by an ordered set of quantum gates, each gate corresponding to a 2^{21} x 2^{21} unitary matrix, where the product **A** of those matrices corresponds to Shor's Algorithm. The final basis-shifted state Ψ_f of the 21-qubit system can then be represented as:

$$\Psi_f = A\Psi_0 = \begin{bmatrix} a_{1,1} & \cdots & a_{1,2097152} \\ a_{2,1} & \cdots & a_{2,2097152} \\ \vdots & \ddots & \vdots \\ a_{2097152,1} & \cdots & a_{2097152,2097152} \end{bmatrix} \Psi_0 \quad (2)$$

Strangely, the final state Ψ_f cannot be measured, nor the amplitudes of its 2^{21} terms deciphered. Instead, each qubit is individually measured in the $\{|0\rangle, |1\rangle\}$ basis, yielding information about the prime factors of the input number. Because most of the "information" in Ψ_f is lost upon measurement, the computation ordinarily must be repeated many times to, for example, build up a useful probability distribution.

Classically, this is a very computationally intense problem because it would require calculating the amplitudes $\{a_{1,1}, a_{1,2}, a_{1,3}, \ldots, a_{2097152,2097152}\}$ in that 2^{21} x 2^{21} unitary matrix **A**. The elements of matrix **A** quantify the entanglements between the 21 qubits caused by their interactions in the gates. And while a modern classical computer certainly could calculate the entanglements among 21 qubits, even 100 qubits already exceed the world's existing computer processing capability because the demands on a classical computer grow exponentially with the number of qubits.

On the other hand, for a quantum computer, that matrix **A** can be effectively applied by subjecting those 21 qubits to approximately 4600 physical quantum gates in the correct order. (Factorizing a larger number requires quantum computer resources that grow polynomially, not exponentially.) The reason that a quantum computer theoretically requires fewer computational resources is that a classical computer must explicitly and individually keep track of all the amplitudes in matrix **A**, while in a quantum computer *nature* keeps track of them in the form of entanglements.[2] Any time we manipulate a qubit, such as by acting on it with a gate, the amplitudes corresponding to its correlations with other entangled qubits get instantaneously manipulated. A single quantum gate, therefore, could manipulate up to 2^{21} amplitudes instantly without a computer having to explicitly perform that many classical calculations.

B. Entanglement: A Double-Edged Sword

In a quantum computer, intentional manipulations of one or more qubits, such as with the use of quantum gates, yield enormous benefits because of the instantaneous updating of correlation amplitudes due to entanglements between qubits. However, *unintentional* manipulations, such as those caused by ambient noise, are just as efficient at instantaneously corrupting those amplitudes.

The primary obstacle in quantum computing is environmental noise or dephasing decoherence. (This is also

[1] All physical qubits are imperfect; each logical (or computational) qubit typically must be encoded by many physical qubits, as will be discussed in greater detail later.

[2] The "information" quantifying those entanglements is not accessible by any measurement, and even the word "information" is a misnomer in this case. Only N bits of information can be extracted from N qubits, even if it may require $\sim 2^N$ amplitudes to describe their entanglements.

true for systems in which an eigenstate of a qubit is an excited state, because the energy relaxation time T_1 is typically much longer than the environmental dephasing time T_2.) Fields and particles permeating the universe tend to interact with qubits and dephase or decohere their coherent superposition states.

All quantum gates take time. Therefore, at any given time t during a computation, the qubits are in a complicated entangled state equivalent to the action of some unitary matrix $U(t)$, so that the vector describing the 21 qubits at time t has up to 2^{21} nonzero complex amplitudes. The more time that elapses, the more opportunities there are for environmental noise to irreparably corrupt entangled qubits.

Entanglement, which is the defining benefit of quantum computing, is a double-edged sword. The good news is that when a gate provides a controlled, known, or intentional change to a qubit, many (or even all) of the amplitudes in the massive state vector immediately change, thanks to Mother Nature, far faster than could be computed classically. The bad news is that *the same thing happens with noise,* such as when random, unexpected, or unintentional interaction occurs between the environment and a qubit. If that noise were to change all or most of the correlation amplitudes, it would crash the quantum computation.

Is there a way to enjoy the benefits of entanglement without the detriments?

C. The Threshold Theorem (Mathematically) Saves the Day

Building on the work of Shor [18], Aharonov and Ben-Or [3] showed, using a simple model based on several strong assumptions, that a quantum computer utilizing qubits and gates having error rates lower than a particular threshold could, with the use of quantum error correction, reduce the computer's error rate to arbitrarily low levels. The so-called Threshold Theorem seems to provide a way out of entanglement's Catch-22: with an unlimited supply of high fidelity qubits and quantum gates configured appropriately, a quantum computer of any size and precision can be built.

The Threshold Theorem depends heavily on quantum error correction ("QEC"); if enough of a computer's qubits are decoupled from each other so that a single error never destroys all the information in the amplitudes, and if the key information is coded in a kind of redundancy that allows detection and correction of that error, then a computer crash may be avoided. QEC depends on encoding a single logical qubit ("LQ") using a system of physical qubits ("PQ") so that the information in the LQ can persist even if and when the information in a single PQ gets corrupted. The QEC code should also be configured to correct the corrupted PQ. One of the more efficient QEC codes requires 7 PQs per LQ [20].

Without QEC, the probability P_s of a quantum computer's success decreases exponentially with size T, where T could refer to the number of gates, number of qubits, total computation time, etc. Because the qubits in a quantum computer are entangled, a single error (caused, e.g., by environmental noise) in the absence of QEC can crash the entire computation; longer computation times, more qubits, and more gates simply increase the opportunity for error, only one of which is required for computer failure. Unruh [23] showed that this problem cannot be solved merely by repeating a noisy quantum computation many times, as "the required number of attempts [to adequately reduce the probability of never finding a coherent outcome]... is exponential in the length [of the input]." To maintain the success probability P_s at a particular desired level, the required accuracy ϵ of individual quantum gates decreases with T. In other words, if we triple the size T of a quantum computation, we must make the quantum gates three times more accurate to maintain the same success rate P_s.

However, using QEC, the probability P_s of a quantum computer's success still decreases with T but not as quickly as without QEC. Specifically, according to Preskill [15], the gate accuracy ϵ necessary to achieve a desired success rate P_s goes as $\epsilon \sim (\log T)^{-b}$ (where typically $3 < b < 4$) versus $\epsilon \sim 1/T$ without QEC.

We can do even better, at least mathematically. In a single-layer QEC code, each LQ is supported by several PQs. However, in a multi-layer *concatenated* code, each top-level LQ is supported by several second-layer LQs, which may each be supported by several third-layer LQs, and so forth, which are ultimately supported by PQs at the bottom layer. Each layer of concatenation provides a reliability boost to the top-layer quantum computation. Indeed, Ref. [3] showed that with concatenated codes utilizing QEC, with error rates of gates and storage below a threshold ϵ_{th}, and under various other assumptions (which will be discussed later), the computer's success probability P_s can be made arbitrarily close to unity. Preskill [15] estimates thresholds ϵ_{th} for gate and storage errors at around 10^{-4}.

Essentially, the Threshold Theorem tells us that, with the use of QEC, it is possible to create a high fidelity LQ out of a sufficiently large number of appropriately configured PQs so long as their gate and storage errors are lower than error threshold ϵ_{th}. The lower their error rates, the fewer PQs are needed to create one LQ.

D. What is a Useful Quantum Computer?

To produce a quantum computer that can solve a particular useful problem, we must know how many LQs are necessary, how many quantum gates to which the LQs are subjected, and how many PQs are necessary for each LQ. For example, for the application of quantum computation to simulating economic price models in derivative securities, Chakrabarti *et al.* [8] estimate a requirement for 10,000 LQs subject to over 3 billion gates. In the case of the most heavily cited application of quantum computing – breaking RSA encryption – Ref. [6] estimates that implementing Shor's Algorithm to factorize a 600 decimal digit number would require more than 10,000 LQs subject to over 600 billion gates.

How many PQs would be required to support each of the necessary LQs? Preskill [15] argues that with error rates ϵ (for both storage and gate) at 10^{-6}, application of Shor's Algorithm would require three levels of concatenation (i.e., $7^3 = 343$ PQs per LQ) and lots of reusable ancilla qubits. (Note that the assumed error rate $\epsilon = 10^{-6}$ is two orders of magnitude lower than his estimated ϵ_{th} and significantly lower than rates that have actually been achieved.) Specifically, he estimates that using Shor's Algorithm to factorize a 600-digit number would require at least 5,000,000 PQs.[3]

It is important to note that, despite theory, not a single LQ using QEC has ever been produced, underscoring the magnitude of the above numbers. As a sort of consolation prize for the lack of any near-term hope[4] to experimentally achieve QEC, Preskill [16] suggests a variety of potential applications for Noisy Intermediate-Scale Quantum systems ("NISQ") that do not utilize QEC. I remain skeptical of both the usefulness of NISQ and the likelihood that anything better will come of it. Further, even if QEC is achieved and a sufficiently large number of LQs are configured to do a useful computation, the number and type of potentially useful computations are still very limited. Aaronson [1], for example, warns over-enthusiastic supporters of quantum computing to beware of caveats.

Therefore, in the remainder of this article, I will address the kind of useful quantum computation that could in theory be achieved by reliably scaling up quantum computers utilizing QEC. That is, I assert that quantum computers must be scalable to ultimately do anything meaningfully useful,[5] and that the possibility of scalability depends in large part on the viability of QEC.

E. The Holy Grail of Fault-Tolerant Quantum Error Correction

Given that QEC is necessary for the scalability of quantum computing, I'll discuss some specifics as well as an example of its implementation. The general idea underlying QEC theory is to transfer entropy of noise to ancilla bits, which are qubits that are not directly related to the LQs performing the desired quantum computation.

With reference to Ref. [20] and [9], let's consider a single LQ whose quantum state we wish to maintain to some accuracy. In a single layer of concatenation, an efficient QEC code that corrects both bit-flip and phase-flip errors requires 7 PQs for that LQ. (In a second layer of concatenation, the LQ would be encoded in 49 PQs, and so forth.) That LQ is initialized to some desired state by encoding its underlying PQs. Then, if a single PQ experiences an error (such as corruption with noise), QEC is applied to correct the error. Finally, the PQs are decoded to yield the final LQ state.[6]

It is important to address when these steps happen. They cannot happen *between* gates, because the QEC process itself requires many gates. Further, the errors that must be addressed by QEC are caused not only by noise and the passage of time, but by the gates themselves. Therefore, quantum gates must act on encoded (or "dressed") qubits. This process is called executing gates "transversally" and is theoretically possible with particular gates (which themselves comprise a universal gate set), establishing the basis of "fault-tolerant" quantum error correction ("FTQEC") [19]. Preskill [15] describes fault-tolerant NOT, Hadamard, Phase, CNOT, and Toffoli gates that can act on encoded PQs.

The QEC code itself is far more complicated and requires several steps, which will be described with reference to an example below: regularly creating fresh ancilla qubits; correlating these ancillas to the LQ; applying syndrome extraction operations; measuring the ancillas (which provide information on *which* PQs were corrupted without measuring or providing information on the state of those qubits); and then correcting the errors using more gates. The following example shows how QEC utilizes "digitization of noise" to correct a random bit-flip error. For simplicity, the LQ will be encoded with only three PQs.

First, the LQ is encoded in a maximally entangled "cat state" of three PQs:

$$a\,|0\rangle + b\,|1\rangle \longrightarrow |\Psi\rangle = a\,|000\rangle + b\,|111\rangle \tag{3}$$

Next, we assume that noise causes a small random rotation to qubit 2 about the X-axis (i.e., a bit flip).[7] For sufficiently small ϵ_2, that noise operator E_2 acts on the LQ to yield:

$$E_2\,|\Psi\rangle = [a\,|000\rangle + b\,|111\rangle] - i\epsilon_2[a\,|010\rangle + b\,|101\rangle] \tag{4}$$

[3] Surface codes are no better. Fowler *et al.* [12] estimate the need for one billion PQs to implement Shor's Algorithm to factorize a 600-digit number. Assuming a PQ error rate just one-tenth of ϵ_{th}, their proposed surface code would require nearly 15,000 PQs per LQ, while the logical ancillas necessary to complete the computation would require an additional 800,000 PQs each.

[4] "Perhaps NISQ will allow us to speed up the time to solution for problems of broad interest in the near future, but we don't know yet whether that will happen."

[5] I ignore the technology of "quantum annealing," which is both possible and very useful, as being improperly characterized as quantum computing.

[6] It is this final state that is actually measured to yield the desired information from the quantum computation. Of course, measurement of the single LQ yields only a single bit of information.

[7] This example was simplified for bit flips (X) but also applies to phase flips (Z).

Next, three ancilla bits in state $|000\rangle$ are entangled with the LQ, after which a syndrome extraction operator S is applied to the system that leaves the original three qubits intact but changes the ancillas according to the location of the error. For example, $S|111\rangle|000\rangle = |111\rangle|000\rangle$, $S|110\rangle|000\rangle = |110\rangle|001\rangle$, $S|100\rangle|000\rangle = |100\rangle|100\rangle$, and so forth. These steps then yield:

$$S(E_2|\Psi\rangle|000\rangle) = [a|000\rangle + b|111\rangle]|000\rangle \\ -i\epsilon_2[a|010\rangle + b|101\rangle]|101\rangle \quad (5)$$

Next, the ancilla bits are measured in the $\{|0\rangle, |1\rangle\}$ basis. If the ancillas are measured in state $|000\rangle$ (which is the most likely outcome), then the measurement projects Ψ to $a|000\rangle + b|111\rangle$, which was exactly its initial (non-corrupted) state. However, if the ancillas are measured in state $|101\rangle$ (with likelihood ${\epsilon_2}^2$), then the measurement projects Ψ to $a|010\rangle + b|101\rangle$. While this is *not* the initial state, knowledge of the ancillas in state $|101\rangle$ tells us that the second bit of Ψ has been flipped, allowing us to correct the error by applying a gate corresponding to an X rotation to qubit 2. Amazingly, this process allows correction of bit flip errors to Ψ without having to measure Ψ. After all, measuring Ψ would project it onto either $|000\rangle$ (with likelihood a^2) or $|111\rangle$ (with likelihood b^2) and destroy its initial superposition state.

A major flaw with the theory underlying QEC digitization of noise, which will be discussed in more detail in Section III, is that it assumes that the noise is, and forever remains, uncorrelated with the environment. That is, in the above example, it assumes that qubit 2 was not *measured* in state $|0\rangle$ or $|1\rangle$.[8] If qubit 2 had indeed been measured (by noise, the environment, a scientist, etc.) in the $\{|0\rangle, |1\rangle\}$ basis, then the LQ would have irreversibly collapsed to either state $|000\rangle$ or $|111\rangle$.

Note that the error described in Eq. 4 *adds* possible eigenstates (four eigenstates versus the two shown in Eq. 3), and the purpose of QEC is to eliminate the extra eigenstates through measurement/collapse of ancillas (and to undo the error if necessary). However, a measurement irreversibly *reduces* the number of eigenstates. QEC, by its nature, simply cannot correct this kind of error.

[8] Steane [20] claims that the digitization of noise of QEC applies equally to projective errors by noise. (Note that "projections" in quantum mechanics are often synonymous with "measurements," but in this case Steane uses the word differently.) However, inherent in his analysis is the assumption that the noise does not impart to the environment information about the projection. These so-called "projective" errors are treated as equivalent to random phase shifts; i.e., they are treated as inherently reversible, in which case no permanent measurement or memory gets embedded in the environment. In other words, Steane assumes that the "projective" event is not a "measurement" event and fails to address that his QEC code would break down if the noise indeed *measured* the qubit.

III. PROBLEMS WITH SCALABLE QUANTUM COMPUTING

A. Questionable Assumptions

The Threshold Theorem and the mathematical foundations of QEC and FTQEC depend on many assumptions, some of which may be entirely unrealistic or technologically unfeasible or may even logically conflict with others. Ref. [9], [10], and [15] discuss some of these assumptions and the extent to which they are reasonable, including:

- Cat states can be prepared – *verifiably* prepared – at the necessary level of concatenation. For example, three levels of concatenation require accurately initializing 343 PQs in maximally entangled state $a|0000\ldots000000\rangle + b|1111\ldots111111\rangle$.
- Essentially unlimited on-demand fresh ancilla bits are available.
- The estimates (of ϵ_{th}, for example) assume maximum parallelism to minimize storage errors.
- Two-qubit gates can act on any pair of qubits.
- Errors are random – i.e., errors are not systemic, common-cause, etc.
- Errors are uncorrelated, or they result in correlations that decay in space and/or time. "Thus when we say that the probability of error per qubit is (for example) $\epsilon \sim 10^{-5}$, we actually mean that, given two specified qubits, the probability that errors afflict both is $\epsilon^2 \sim 10^{-10}$. *This is a very strong assumption.*" (Ref. [15], emphasis added.)

I will argue in Section IIIC that the last assumption is the most concerning and that Preskill's characterization of it as "very strong" has been severely underappreciated in the field.

B. Skepticism of Quantum Error Correction

Researchers have identified several other fundamental problems that serve to discredit the assertion that quantum computing is scalable. First, Dyakonov [10] correctly points out that QEC has never been achieved at *any* level of concatenation.[9] The only evidence that QEC is physically possible consists of theoretical and mathematical demonstrations which, as discussed above, rest

[9] Ofek *et al.* [14] claim to have experimentally demonstrated QEC by showing an example in which the lifetime of a qubit exceeds the lifetime of the system's constituents. For many reasons that exceed the scope of this paper, their argument, while interesting, utterly fails.

on a lengthy list of questionable and potentially mutually conflicting assumptions. Like the *theoretical* physical reversibility of scrambling an egg, the potential for scalable quantum computing may rest on mathematical assumptions that are at odds with our actual observations of the world.

Second, there appear to be logical inconsistencies between mathematical theorems and physical reality. For example, Alicki [4] argues that the Threshold Theorem assumes physically unrealistic infinitely fast gates. Further, Hagar [13] shows that three assumptions of FTQEC are logically contradictory: a) errors are uncorrelated; b) gates can be executed in time scales of the Rabi frequency; and c) unlimited on-demand fresh ancilla bits are available. A theorem that rests on conflicting statements is necessarily false.

Third, Waintal [24] points out that every error code is inherently limited to some set of "correctable" errors, and no code can address all errors. Further, he suggests one type of error – a "silent stabilizer failure" in which a stabilizer is not measured for several clock cycles – that places a lower limit on the precision η_L of logical qubits in a surface code: "[I]t is sufficient that a single stabilizer failure occurs for the duration of one logical operation to produce an irreversible logical failure, irrespectively of [the number of physical qubits]." He calculates that a quantum computation will crash unless the probability is less than 10^{-20}, while its real-world probability could actually be 15 orders of magnitude higher.

Fourth, there may be evidence that popular belief in the viability of QEC and scalable quantum computing is partly a product of exaggerated and false claims. Many publications claim directly or indirectly that QEC has already been experimentally realized or that QEC requires far fewer PQs per LQ than what careful estimates suggest. For instance, Ref. [21] misleadingly characterizes QEC as "typically incurring 10-50 physical qubits to encode one fault-tolerant qubit." Recent statements by two of quantum computing's most well-known supporters are telling. Preskill [16] said, "[T]he era of fault-tolerant quantum computing may still be rather distant," and Aaronson [2] said, "It's genuinely gotten harder to draw the line between defensible optimism and exaggerations verging on fraud."

C. The Measurement Problem Strikes Back

Setting aside the above concerns, the primary problem plaguing the potential for scalable quantum computing is this: **the words "noise" and "measurement" are treated with a double standard in quantum computing theory.** Specifically, quantum computing theory assumes (and needs) measurement at the end of computation but ignores it *during* the computation. Further, it assumes that noise does not necessarily measure[10] but scientists do. As shown in Section IIE, digitization of noise can only correct an error caused by noise that does not measure a qubit, while the computer's state at the end of a computation only yields information when a user measures it. The distinction here is artificially imposed by theorists, because Mother Nature does not distinguish between noise and scientists. Sometimes, noise measures.

The Measurement Problem manifests itself further in the assumption (Section IIIA) that errors result in random and uncorrelated phase shifts (or equivalently, through Hadamard gates, bit flips), or that they result in correlations that decay in space and/or time. This assumption implies and requires that the environment retains no "memory" of these interactions – for example, a photon bounces off and correlates to a qubit but the interaction itself provides no permanent information to the environment as to the qubit's state. Thus, the kinds of errors assumed by the Threshold Theorem are those in which the environment does not make any permanent measurement.[11] This may certainly be true of some errors, but there is no logical or scientific basis to make this assertion about all errors.

This assumption guarantees that errors are *reversible* noise, which is convenient for quantum computing theory because QEC cannot correct or undo an irreversible measurement. The noise models used to bolster the credibility of QEC theory literally assume that interactions with the environment that occur during the computation are reversible (i.e., not measurements), while interactions with the environment that occur at the end of the computation are irreversible measurements, with no logical, mathematical, or scientific justification.

The universe is inundated with objects, particles, and fields that constantly interact. Human scientists themselves and their measuring devices constantly emit, absorb, and deflect molecules, photons, etc., that interact with each other, the environment, and the objects of measurement. Indeed, every measurement – notably of quantum phenomena – begins with an interaction of the object of interest with the environment. The measuring device amplifies that interaction so that the scientist can distinguish a measurement outcome. Note that the measuring device has no monopoly on its ability to amplify microscopic interactions. The environment itself is very effective at amplifying microscopic interactions, as well demonstrated by chaos theory and simulations.[12] Rather, the scientist's measuring device is one that is designed to amplify particular interactions in particular

[10] The noise models used to simulate environmental decoherence choose noise interactions that are uncorrelated to each other and the environment and therefore are inherently reversible.

[11] If one perfectly reverses a "measurement" so that there is no lasting evidence, then there was actually no measurement [26].

[12] Boekholt *et al.* [7] provide a fascinating discussion of the ability of chaos to eradicate predictability of enormous black holes even to initial conditions specified to within the Planck length.

ways that allow the scientist to distinguish outcomes of interest.

If all measurements are initiated by environmental interactions, then what is noise? The word "noise" is nothing more than the word given to environmental interactions that the scientist does not like or want – e.g., because he has not accounted (or cannot account) for them in his calculations. In other words, among an object's constant interactions with particles and fields in its environment, a human scientist using a measuring device to measure some aspect of the object will classify some of these interactions as "noise," but the distinction is an artificial one that is not acknowledged or respected by Mother Nature.

We know with absolute certainty that quantum events at least *sometimes* correlate to their environment, otherwise irreversible measurements would not be possible and the necessary last step in any quantum computation would likewise be impossible. A quantum computer scientist relies on a specially configured measuring device, at the end of a quantum computation, to amplify the computer's inevitable interactions with its environment.

The most fundamental (and, I believe, unsolvable) problem for scalable quantum computing is that the noise models used to validate QEC assume by necessity that environmental interactions that occur during the quantum computation do not correlate – or, at least, do not *permanently* correlate in the case of correlations that decay with time and/or space – with the environment, but environmental interactions that occur at the end of the computation do. That is, the universe's "noise" does not irreversibly measure during computation but does so at the end. There is, quite simply, no logical or scientific justification for the conveniently inconsistent uses of the words "noise" and "measurement."

In the same vein, Hagar [13] argues that we are treating entanglement with a double standard by assuming that error correlations decay but inter-qubit correlations don't. Imagine N qubits in a quantum computer that are all highly entangled with complicated inter-qubit correlation amplitudes that are represented in a 2^N x 2^N matrix (like matrix $\mathbf{A}$ in Eq. 2 for a 21-qubit system). The beauty of quantum computing is that by subjecting a single qubit to a quantum gate (or two qubits to a two-qubit gate), *all* of the relevant amplitudes in the quantum state vector are instantaneously updated. Indeed, this simple but incredible fact entirely explains the computational speedup over classical computers. In other words, the theory of quantum computing assumes that when a qubit interacts with a gate or another qubit (i.e., something that the human user would not characterize as "noise"), it is already correlated to lots of other qubits due to preexisting entanglements, and the system's state vector after the interaction depends both on that interaction as well as the qubit's history of entanglements.[13] In that sense, all entangled qubits "inherit," via changes in their inter-qubit correlation amplitudes, information about each qubit's interactions.

However, noise is treated very differently. A particle of environmental noise, by the same logic, should already be correlated to lots of other environmental objects due to its own history of entanglements with them. Therefore, by the same logic, an interaction between that noise particle and a qubit should not only instantaneously update the quantum computer's inter-qubit correlation amplitudes, but should in fact instantaneously update the environment's inter-particle correlation amplitudes too.[14] Because such a change in amplitudes among environmental particles could be measured in a well-designed experiment – that is, the evidence of the interaction gets immediately and permanently embedded in the environment – such an interaction represents an irreversible measurement. If it occurs at any time during the quantum computation, the computer will crash.

This fact is well known in the field, which is why QEC models consider only "noise" whose interaction with a qubit does *not* instantaneously update the environment's inter-particle correlation amplitudes. Noise that is simply uncorrelated with the environment or other noise, or whose correlations decay over time or space, is the gold standard of QEC. While some noise certainly meets one of these criteria, the assumption that all noise interacting with a quantum computer will do so has absolutely no basis in empirical evidence.

Hagar [13] characterizes this problem well: "[I]f one is allowed to cheat just once in quantum mechanics, one can indeed do miracles." Ultimately, Preskill's [15] concern that errors in QEC are assumed to be uncorrelated, or that they result in correlations that decay in space and/or time, was well-founded and may prove an insurmountable obstacle to scalable quantum computing.

IV. A DIFFERENT APPROACH

The failure of theorists to fully address noise that irreversibly measures qubits is fatal to QEC theory and any prospects for scalable quantum computing. To further underscore the physical difficulties inherent in scaling up a quantum computer to a useful size, I'll discuss a hypothetical quantum computer based on "position qubits" and its parallels to the classic double-slit interference experiment.

---

[13] The history-dependence of the state vector is reflected in the fact that the quantum computation can be represented by a unitary operator.

[14] Mathematically, the state vector representing the entirety of the environment and the quantum computer instantaneously updates, by the single interaction, to reflect nonzero correlation amplitudes between most, if not all, of the qubits and most, if not all, of the environmental particles.

A. Double-Slit Interference Experiments

A double-slit interference experiment ("DSIE") is perhaps the most fundamental and most demonstrative of quantum mechanics. DSIEs have been used to demonstrate quantum interference effects on individual fermions, beginning with the Davisson and Germer experiment on electrons in 1927, all the way up to molecules comprising hundreds of atoms [11].

Performing a DSIE on an object requires placing the object in a "cat" superposition state over distinct position eigenstates and then maintaining that state long enough to show interference effects. The position eigenstates are typically separated by a distance greater than the object's dimension, otherwise the two slits in the "double slit" would not distinguish them.

In practice, a DSIE is performed on an object by first passing the object through a hole or slit to localize the object to within some dimension Δx, which causes the object's wave packet to disperse in a manner that satisfies quantum uncertainty: $\Delta x(m\Delta v) \geq \hbar/2$. A double-slit plate (having slits separated by distance d) is placed sufficiently downfield from the localizing hole that the object's dispersed wave is wider than distance d and illuminates both slits. The two slits allow only two parts of the object's wave to pass; those parts represent the "cat" state of the object.

If a photon having a wavelength $\lambda < d$ (so that it can distinguish the two slits) were to measure the object immediately after traversing the double-slit plate, the object would be found entirely localized at either one slit or the other. If, however, a detector screen is placed sufficiently downfield from the double-slit plate (and any intervening measurement prevented), then the object will be detected in a location that is consistent with its *not* having been localized at one slit or the other of the double-slit plate. In fact, every DSIE ever performed on matter (i.e., fermions) has depended on dispersion of its quantum wave packet via quantum uncertainty as described above.

Demonstrating quantum interference effects of an object in a DSIE requires maintaining coherence in the object's superposition state as the object traverses from the localizing hole to the detection screen. Any unintended interaction with a particle or field during the DSIE will decohere that superposition. Unfortunately for DSIEs, objects, particles, and fields pervade the universe and are constantly interacting with each other and decohering superpositions.

Electrons can easily demonstrate interference effects in a DSIE for two reasons. First, their small size makes them difficult targets for decohering noise. Second, their small mass allows their wave packets to disperse more quickly, giving decohering noise less time to interact with them. Similarly, as the size of an object grows, the likelihood of a decohering interaction during a potential DSIE increases in two ways: more time is needed for the object's wave packet to adequately disperse, but less time is available between decohering impacts with noise because of the object's larger cross section. To the extent that an object's interaction cross section is proportional to its mass, the number of potentially decohering interactions during a DSIE increases as the square of the object's mass.

In other words, the time needed to perform a DSIE on an object (which depends on quantum dispersion to produce an appropriate superposition) increases with the number/mass of its (entangled) particles; and the time needed for environmental noise (e.g., particles and fields throughout the universe) to prematurely decohere a superposition decreases with the number/mass of (entangled) particles. Therefore, the probability P of a molecule of mass m surviving long enough to create a cat state and demonstrate interference is an exponential decay in m^2: $P \sim e^{-m^2}$.

The net result of this analysis is that nature makes it increasingly difficult at increasing rates to do DSIEs on larger objects.[15] For instance, could a DSIE be done on a dust particle? Tegmark [22] calculates coherence lengths l_c (roughly "the largest distance from the diagonal where the spatial density matrix has non-negligible components") for a $10\mu m$ dust particle caused by various decoherence sources. For a dust particle floating around in Earth's atmosphere at 300K, Tegmark calculates a coherence length of $10^{-17}m$, which is 12 orders of magnitude smaller than the dust particle itself. The dust particle is impacted so frequently by decohering air molecules that its wave packet never disperses by more than a trillionth of what would be necessary to pass through a double-slit plate.

But what about that same dust particle in deep, dark space, far from the radiation or gravity of any stars? Tegmark calculates that cosmic microwave background (CMB) radiation alone will localize the dust particle to within 1/1000 of its size. Even there, far from most evidence of a noisy universe, a DSIE on a dust particle is destined to fail. Whether or not some engineering solution could, in principle, allow for a DSIE demonstration on a dust particle, what is certain – and what I believe is undisputed – is that it is not technologically feasible to perform a DSIE on a dust particle or anything even close to it.

In the past century, despite enormous efforts and expense, the largest object subjected to a DSIE was an 810-atom molecule [11]. If $P \sim e^{-m^2}$, how infeasible or expensive will it be to do a DSIE on an object with a million fermions? A billion fermions? Extremely, if such an experiment is physically possible at all.

[15] On this basis alone, I would argue that DSIEs are not "scalable," because the difficulty or expense of doing a DSIE does not scale polynomially with the object's size.

B. DSIE Parallels to Quantum Computing

Consider a hypothetical "position qubit." The position of a fermion is used as the basis of a position qubit, so that its state is a superposition of position eigenstates $|0\rangle$ and $|1\rangle$ corresponding to semiclassical localizations separated by some distance d. There are dozens – perhaps hundreds – of proposals for physical implementations of qubits, and there is no physical reason that the position of a fermion over two distinct positions cannot be the basis for a quantum bit. There is also no physical reason why multiple position qubits cannot be entangled with well-understood quantum gates, like Hadamard, CNOT, Toffoli, and so forth.[16]

As discussed in Section IID, realistic estimates suggest that a useful quantum computer will need at least a million to a billion physical qubits (e.g., 10,000 LQs each encoded by 10,000 PQs). To build a useful quantum computer out of position qubits, then, the computer will ultimately need to be able to controllably entangle most or all of these qubits. That capability is significantly more difficult, technologically, than the ability to create a simple cat state.

But a cat state, in the case of a quantum computer using position qubits, is identical to the state produced in a DSIE. Crucially, creating a cat state in a quantum computer having 10^6–10^9 position qubits is *at least as technologically and economically unfeasible* as performing a DSIE on an object with 10^6–10^9 fermions. Of course, a quantum computer must do much more than create a cat state. The entanglements between the position qubits must be controllable in a way that allows for quantum computation and processing, a monumental capability that dwarfs the ability to create a cat state.

Setting aside the overwhelming (and prohibitive) technological hurdles to building a useful position-qubit quantum computer, assume for the moment that the computer has been built and it has just created a maximally entangled cat state of N fermions. Then, some environmental particle (which the scientist would call "noise") having coherence width w gets absorbed by qubit K, causing its trajectory to change.

- If $w > d$, then no information gets transmitted about the qubit's state. This is the kind of error that could potentially be addressed by QEC.
- If $w < d$, then the particle's absorption by qubit K distinguishes the qubit's state by embedding its position information into the environment. Any and all other measurements of the other qubits in the cat state will perfectly correlate to the position of qubit K, which means that the cat state will be irreparably destroyed. QEC *cannot* fix this error (an unintentional measurement) for the same reason that it cannot restore a quantum state after an *intentional* measurement at the end of a computation.

Assuming that all environmental noise is, or can be restricted to, particles with a sufficiently long coherence length is useful for QEC theory but is scientifically unfounded. Some noisy photons will inevitably satisfy $w < d$, a fact that will render QEC impotent against environmental threats to position-qubit quantum computation.

Because this is the same mechanism that afflicts DSIEs, the hypothetical example of a position-qubit quantum computer demonstrates several points. First, there is a practical/cost limit to the number of entangled "position qubits," rendering the possibility of controllably entangling a million to a billion position qubits (which is what would be necessary to achieve usefulness) remote at best. Second, a quantum computer based on position qubits is not scalable for the same reason that DSIEs are not fundamentally scalable. Finally, QEC will not work on such a computer because some environmental noise will inevitably be capable of distinguishing a qubit's eigenstates.

The parallels between DSIEs and the above hypothetical quantum computer are both suggestive and instructive. A DSIE is perhaps the most fundamental demonstration of the nature of the quantum world, yet a quantum computer that mirrors its function and design is neither scalable nor correctable using QEC. While some may retort that a "position qubit" is just a bad example of a qubit, I would argue that its close relationship to DSIEs tells us something fundamental about both the quantum world and the unscalability of quantum computers.

V. CONCLUSIONS

The theory underlying quantum computing and quantum error correction applies a fatal double standard to the words "noise" and "measurement." Interactions with qubits at the end of computation are treated as "measurement" that irreversibly project onto the $\{|0\rangle, |1\rangle\}$ basis; however, interactions during computation are not. Instead, noise is modeled and generally assumed to be random and uncorrelated and providing no (permanent) information to the environment regarding a qubit's state, allowing its effects to be reversed under certain conditions. However, there is no logical or scientific justification for treating all environmental interactions during a computation as inherently reversible and at least some such interactions at the end of a computation as irreversible measurements. The failure of quantum computer theory to adequately address the self-conflicting treatments of noise and measurement makes it suspect.

Quantum computers, like double-slit interference experiments, depend on the demonstration of quantum in-

[16] I don't know *how* to so entangle them, so I will follow the example of quantum computer theorists and defer to future quantum computer engineers.

terference effects. DSIEs demonstrate that sometimes noise makes actual – i.e., permanent and irreversible – measurements. This kind of noise renders DSIEs unscalable because the rate of such interactions increases as the square of an object's mass. To the extent that the mechanism that limits the scalability of DSIEs is fundamental to the quantum world (as opposed to a quirk of DSIEs), the combination of quantum entanglement with noisy/unintended projective measurements may similarly limit the power of quantum computers.

The scalability of quantum computers depends on creating systems of larger and larger size that are: a) highly and controllably entangled; and b) reversible (until the scientist's final intentional measurement). DSIEs are not scalable in practice, even if the assumption of universality of quantum mechanics implies that DSIEs are scalable in principle. If there is something fundamental about the physical world that makes it practically impossible to create highly entangled reversible systems larger than a few thousand particles, and if a useful quantum computer requires at least a million physical qubits, then useful quantum computing is effectively impossible.

Finally, the example of the hypothetical "position qubit" quantum computer is suggestive. It was shown to be neither scalable nor subject to quantum error correction. Either a position qubit is a poor example of a qubit, or the example computer highlights that unintended projective measurements by objects and fields ubiquitous in the universe, which present a fundamental scalability problem in DSIEs, also present a fundamental scalability problem in quantum computing.

ACKNOWLEDGMENTS

I would like to thank Scott Aaronson, Kenneth Augustyn, Martin Bier, David Chalmers, Michael Dascal, Michel Dyakonov, Amit Hagar, Gary Ihas, Annie Knight, Christopher Lind, Andrea Mari, Kyle Padgett, Brian Pitts, Douglas Porpora, Igor Salom, Javad Shabani, Paul Tappenden, and Xavier Waintal for their guidance, comments, and stimulating conversations. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

[1] Aaronson, S., 2015. Read the fine print. *Nature Physics,* 11(4), pp.291-293.

[2] Aaronson, S., 2021. QC ethics and hype: the call is coming from inside the house. https://www.scottaaronson.com/blog/?p=5387

[3] Aharonov, D. and Ben-Or, M., 2008. Fault-tolerant quantum computation with constant error rate. *SIAM Journal on Computing.*

[4] Alicki, R., 2006. Quantum error correction fails for Hamiltonian models. *Fluctuation and Noise Letters,* 6(03), pp.C23-C28.

[5] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J.C., Barends, R., Biswas, R., Boixo, S., Brandao, F.G., Buell, D.A. and Burkett, B., 2019. Quantum supremacy using a programmable superconducting processor. *Nature,* 574(7779), pp.505-510.

[6] Beckman, D., Chari, A.N., Devabhaktuni, S. and Preskill, J., 1996. Efficient networks for quantum factoring. *Physical Review A,* 54(2), p.1034.

[7] Boekholt, T.C.N., Portegies Zwart, S.F. and Valtonen, M., 2020. Gargantuan chaotic gravitational three-body systems and their irreversibility to the Planck length. *Monthly Notices of the Royal Astronomical Society,* 493(3), pp.3932-3937.

[8] Chakrabarti, S., Krishnakumar, R., Mazzola, G., Stamatopoulos, N., Woerner, S. and Zeng, W.J., 2021. A threshold for quantum advantage in derivative pricing. *Quantum*, 5, p.463.

[9] Dyakonov, M.I., 2006. Is fault-tolerant quantum computation really possible?. *Future Trends in Microelectronics. Up the Nano Creek,* p.4.

[10] Dyakonov, M.I., 2020. *Will we ever have a quantum computer?.* Springer.

[11] Eibenberger, S., Gerlich, S., Arndt, M., Mayor, M. and Tüxen, J., 2013. Matter–wave interference of particles selected from a molecular library with masses exceeding 10000 amu. *Physical Chemistry Chemical Physics,* 15(35), pp.14696-14700.

[12] Fowler, A.G., Mariantoni, M., Martinis, J.M. and Cleland, A.N., 2012. Surface codes: Towards practical large-scale quantum computation. *Physical Review A,* 86(3), p.032324.

[13] Hagar, A., 2009. Active Fault-Tolerant Quantum Error Correction: The Curse of the Open System. *Philosophy of Science,* 76(4), pp.506-535.

[14] Ofek, N., Petrenko, A., Heeres, R., Reinhold, P., Leghtas, Z., Vlastakis, B., Liu, Y., Frunzio, L., Girvin, S.M., Jiang, L. and Mirrahimi, M., 2016. Extending the lifetime of a quantum bit with error correction in superconducting circuits. *Nature,* 536(7617), pp.441-445.

[15] Preskill, J., 1998. Fault-tolerant quantum computation. In *Introduction to quantum computation and information* (pp. 213-269).

[16] Preskill, J., 2018. Quantum Computing in the NISQ era and beyond. *Quantum,* 2, p.79.

[17] Feynman, R.P., 1982. Simulating Physics with Computers. *International Journal of Theoretical Physics,* 21(6/7).

[18] Shor, P.W., 1994, November. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Anual Symposium on Foundations of Computer Science* (pp. 124-134). IEEE.

[19] Shor, P.W., 1996, October. Fault-tolerant quantum computation. In *Proceedings of 37th Conference on Foundations of Computer Science* (pp. 56-65). IEEE.

[20] Steane, A.M., 2007. A tutorial on quantum error correction. In *PROCEEDINGS-INTERNATIONAL SCHOOL OF PHYSICS ENRICO FERMI* (Vol. 162, p. 1). IOS

Press; Ohmsha; 1999.

[21] Tannu, S.S. and Qureshi, M.K., 2019, April. Not all qubits are created equal: a case for variability-aware policies for NISQ-era quantum computers. In *Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems* (pp. 987-999).

[22] Tegmark, M., 1993. Apparent wave function collapse caused by scattering. *Foundations of Physics Letters,* 6(6), pp.571-590.

[23] Unruh, W.G., 1995. Maintaining coherence in quantum computers. *Physical Review A,* 51(2), p.992.

[24] Waintal, X., 2019. What determines the ultimate precision of a quantum computer?. *Physical Review A,* 99(4), p.042318.

[25] Zhou, Y., Stoudenmire, E.M. and Waintal, X., 2020. What limits the simulation of quantum computers?. *Physical Review X,* 10(4), p.041038.

[26] Żukowski, M. and Markiewicz, M., 2021. Physics and Metaphysics of Wigner's Friends: Even Performed Premeasurements Have No Results. *Physical Review Letters,* 126(13), p.130402.