Random potentials can cause quantum particles to localize, that is, to remain in a finite region of space instead of diffusing [1–3]. In three dimensions and at fixed energy (and for specific lower-dimensional systems), this effect only occurs after some critical disorder is reached, resulting in a second-order phase transition — the Anderson localization transition [4]. Physically, this is a transition between a conductor and an insulator. Numerical access to this transition is hampered by the large Hilbert spaces needed in the limit of large volumes. Additionally, it is unclear to what extent the transition is affected by the presence of interactions [5, 6]. Localization is a purely quantum mechanical phenomenon caused by interference among different paths. It is perhaps not surprising then that a quantum computer is particularly well suited to capture its physics. The purpose of this paper is to flesh out a method to study localization in quantum computers with a number of qubits scaling as the logarithm of the size of the lattice, opening up the prospect of useful physical simulation with a small number of (corrected) qubits.

We begin by considering the Anderson tight-binding Hamiltonian to be localized, and the medium becomes non-vanishing disorder $W$. In the limit $W = 0$, this is a free theory, in which all eigenstates are delocalized. The only tunable parameter is $W$, the disorder parameter. In the limit $W = 0$, this is a free theory, in which all eigenstates are delocalized. Macroscopic properties of this model — those apparent in the limit of large volumes — do not depend on the particular instantiation of $u_i$. The most interesting such property is localization: in one and two dimensions, any non-vanishing disorder $W$ causes all eigenstates of the Hamiltonian to be localized, and the medium becomes an insulator. In three dimensions, the medium remains a

$$H_{\text{site}} = -\sum_{\langle ij \rangle} (c_i^\dagger c_j + \text{h.c.}) + W \sum_i u_i c_i^\dagger c_i.$$ (1)
conductor up to a critical disorder $W_c \approx 16.5$ [21], above which all states are again localized. This phase transition in three dimensions is an easy target for quantum simulation.

We first discuss the proposal in the context of one-dimensional model and then indicate how to extend it to higher dimensions. To simulate the Anderson tight-binding model in a single dimension, interpret each element of the computation basis as a binary integer specifying the position of the site $(0 \ldots (L-1))$ occupied by the electron. Thus, $|01101\rangle$ is the state of the system when the electron is at site 13 — we will abbreviate this state as $|13\rangle$. The time evolution is Trotterized, and the effects of the kinetic $H_K = -\sum_{<ij>}\left(c_i^\dagger c_j + \text{h.c.}\right)$ and potential $H_V = W \sum_i u_i c_i^\dagger c_i$ terms are implemented sequentially:

$$e^{-iHt} \approx (e^{-iH_K \Delta t} e^{-iH_V \Delta t})^{1/\Delta t}. \quad \text{(2)}$$

In this formulation of the Anderson model, the kinetic Hamiltonian $H_K$ could be diagonalized by a quantum Fourier transform; however, this is no longer the case when the disorder lies on the links, as in a model discussed below. Because of this we instead simulate the evolution of $H_K = H_{K,e} + H_{K,o}$ by splitting it into even ($H_{K,e}$) and odd ($H_{K,o}$) links. Since $H_{K,e}$ and $H_{K,o}$ commute there is no error arising from this Trotterization. The Hamiltonian of the even links couples sites that differ only in the last qubit

$$H_{K,e} = |0\rangle \langle 1| + |2\rangle \langle 3| + \cdots + \text{h.c.} = I^{\otimes (V-1)} \otimes \sigma_x, \quad \text{(3)}$$

and $e^{-iH_{K,e} \Delta t}$ is therefore simulated by a rotation about the $X$ axis of the least-significant qubit. The evolution of the odd links appears more complicated, but is simplified by first translating the entire lattice by 1. By this translation, odd links are transformed into even links. After the shift, time-evolution under $H_{K,e}$ is performed again, followed by a shift back into place. The resulting circuits for evolving $e^{-iH_K \Delta t}$ are shown in Figure 1.

Having evolved with $H_K$, we come to the crux of our proposal: evolving under the disordered potential

$$H_V = W \sum_i u_i |i\rangle \langle i|. \quad \text{(4)}$$

The evolution under $H_V$ requires the phase of the state to be changed by the same random number every time the particle finds itself at a particular lattice site (which corresponds to a state in the computational basis). That means that the same random number has to be generated multiple times. Determining the random values $u_i$ classically and constructing a circuit using them would necessitate $O(V)$ gates in the time-evolution, but with a different approach we can obtain a cost merely polynomial in the volume. We first observe that with standard methods on a classical computer, the $u_i$ are typically not truly random variables, but instead are defined to be the output of a pseudo-random number generator (PRNG) — a circuit sufficiently complicated so that the $u_i$ look random to any practical statistical test. Therefore, we will define $H_V$ to be specified by the output of a particular seekable PRNG, and use that circuit directly in the time evolution.

A seekable PRNG is a PRNG from which the $i$th element $f(i)$ can be obtained in constant time, independent of the value of $i$. This contrasts with the PRNGs used in most computer simulations, in which elements must be calculated sequentially, so that calculating $f(i)$ requires $O(i)$ steps. Given a short (logarithmic in the number of bits $Q$ used to represent $i$) classical circuit computing a PRNG $f$, one can readily produce a quantum circuit implementing a unitary $U_f$ defined by $U_f |i\rangle |0\rangle = |i\rangle |f(i)\rangle$. Taking the output of the PRNG to define the site disorder by $u_i = 2^{-Q} f(i)$, so that

$$H_V = W \sum_i \frac{1}{2^Q} f(i) |i\rangle \langle i|, \quad \text{(5)}$$

we see that evolution under $H_V$ can be obtained by first applying $U_f$ to compute the PRNG, performing a diagonal phase rotation by the amount specified by the value in the ancillary register, and then applying $U_f^\dagger$.

The setup above requires the construction of a suitable $f(i)$. Seekable PRNGs are often defined via cryptographic hash functions like SHA256 [22]. In this construction, a sequence of $K$ PRNGs indexed by seeds $k$ are constructed via $f_k(i) = \text{SHA256}(i \ast K + k)$. This construction is known to perform very well [23], but cryptographic hashes typically operate on fixed-size registers of large numbers of bits, and the well-studied ones are therefore unobtainable on near-term quantum computers. For this reason, we instead define a seekable PRNG with a random classical circuit — that is, a random permutation matrix.

A random permutation matrix $P$ may be used to define a seekable PRNG via $P |i\rangle = |f(i)\rangle$. This introduces weak correlations between the different values of $f(i)$, as $f(i) \neq f(j)$ whenever $i \neq j$; these correlations are unmeasurably in the large volume limit, and we will ignore them.

\begin{figure}[h]
\centering
\includegraphics[width=0.8\textwidth]{time-evolution-circuits}
\caption{Time-evolution circuits for the Anderson tight-binding model with site disorder, on eight sites. On top is shown approximate evolution under the kinetic Hamiltonian $H_K$; on the bottom is the evolution under the disordered potential $H_V$. The construction of the random permutation $P$ is discussed in the text.}
\end{figure}
It remains to construct a random permutation operator on a quantum computer. Our method will be to add randomly a number of NOT and TOFFOLI gates on an extended register with \( Q + (Q - 3) \) qubits. It is easy to see this generates a random permutation with a probability independent of the permutation. Indeed, with the aid of \( Q - 3 \) extra ancillary qubits, any permutation matrix can be obtained by composing the NOT and TOFFOLI gates [24]. Beginning with an empty circuit (corresponding to the identity), consider the process of appending one randomly-selected gate at a time (the probability of picking any of the NOT or TOFFOLI gates is irrelevant as long as it does not vanish for any of them). This is a Markov chain in the space of permutations which, by virtue of Toffoli’s construction, is ergodic. As long as one of the gates included is the identity gate, it is also aperiodic, and therefore the chain converges to the unique stationary distribution where every permutation is equally probable. Therefore, a sequence of \( G \) randomly selected NOT and TOFFOLI gates will converge to a random permutation matrix as \( G \to \infty \). This is true regardless of the distribution of gates used, although the distribution does affect the rate of convergence. As one additional simplification, for our demonstrations we dispense with the anciliaries which are required to sample a truly random permutation matrix. This modification makes no difference in the large-volume limit. To see this, relabel the highest-order half of the qubits, representing the least-significant digits, as ancillary. These qubits contributed very little to the energy level of a site, so this change disappears in the infinite-volume limit.

Although we have shown that with enough random gates this construction will yield random numbers, it is important that the number of gates required scales polynomially, rather than exponentially, with \( Q \). To demonstrate that this is the case, we run the dieharder [25] battery of statistical tests (based on the diehard tests [26]) on random numbers generated by random classical circuits on 30 bits. As dieharder takes in a sequence of 8-bit numbers, we truncate each random number to the highest-order 8 bits. Trying different lengths of gates, we find that 600 gates is sufficient to consistently pass all statistical tests in the battery. Similarly, for random classical circuits on 50 bits, we find 1200 gates to be sufficient, and for 100 bits 2600 gates. This is suggestive of low-exponent polynomial scaling.

The resulting circuit for evolving a three-qubit (eight-site) model under \( H_V \) is shown in Figure 1.

The generalization of our algorithm to higher dimensions is straightforward. The random potential in the Hamiltonian is local and makes no reference to the spatial structure of the lattice, and so that portion of the time evolution is unaffected by the number of dimensions. The kinetic Hamiltonian factorizes, and we have in three dimensions

\[
H_V^{(3)} = H_K \otimes I \otimes I + I \otimes H_K \otimes I + I \otimes I \otimes H_K,
\]

so that kinetic evolution may be performed independently in each dimension separately.

This completes the construction, on a digital quantum computer, of the time evolution operator \( e^{-iHt} \). Many experiments can be performed once this time-evolution is available. The most natural is to begin with an electron at a particular site (\( |\Psi(t = 0)\rangle = |0\rangle \)) and measure its propagation in time. The two possible qualitative behav-
D/L which is equivalent in the infinite-volume limit to the maximum \( D \). Thus, preparing the state \( |0\rangle \) (or any other basis state), evolving for a long time, and finally measuring the position of the electron, informs us which phase we are in. In practice, we plot \( D/L \), which is \( 0 \) in the infinite volume limit of the insulating phase and a finite constant in the conducting phase. Such a plot, computed classically, is shown in Figure 3; note that the results with random circuits (as discussed above) agree with those obtained using a conventional PRNG.

This method cannot yet be implemented at scale on a quantum computer; achieving quantum advantage would require about 50 fault-tolerant qubits, which are not yet available. The state of what is currently achievable is depicted in Figure 4. With publicly available quantum computing facilities provided by Rigetti, we are able to simulate around 10 time-steps with 4 sites before noise and decoherence entirely take over.

The site disorder of Eq. 1 is not the only way to introduce disorder onto the lattice. Another option is to introduce the disorder on the hopping terms:

\[
H_{\text{link}} = \sum_{\langle ij \rangle} (W_{ij} - 1) \left[ c_i^\dagger c_j + \text{h.c.} \right]
\]  

(8)

In this model the link between \( i \) and \( j \) has an associated random variable \( u_{ij} \), and there is no potential on the sites. To evolve this Hamiltonian we may use a similar strategy as before. In one dimension, two random permutation matrices on \( Q-1 \) qubits are constructed. They determine the disorder on even and odd links, respectively. The circuit for performing evolution under this Hamiltonian is shown in Figure 5.

We have discussed site-disorder and link-disorder on cubic lattices of arbitrary dimension. In general, a Hamiltonian which is sparse and efficiently row-computable (a short circuit can be presented to compute the non-zero entries in any row of the Hamiltonian) can be simulated in time logarithmic in the dimension of the physical Hilbert space [27]. The trick used in this paper is quite general: when considering a model with many random values in the Hamiltonian, those values may be defined to be the output of a PRNG without changing the macroscopic properties of the model. This removes the need to specify \( O(V) \) values explicitly in a circuit, and allows efficient simulation of the Hamiltonian.

The algorithms presented here allow the physics of metal-insulator transitions to be accessed with a number of qubits scaling with the logarithm of the volume of the system. These do require fault-tolerant qubits, which have not yet been demonstrated in practice. However, about 50 such qubits would already allow quantum computers to push past the systems that can be treated with a classical computer.

Besides going to larger volumes than a classical computer could hope to achieve, the gentle scaling of resources with Hilbert space opens up the possibility of studying few-body interactions in random potentials as well as Anderson transitions in higher dimensions, with an eye toward determining the upper critical dimension [28].

![Figure 4](image-url)  

**FIG. 4.** Average distance, as measured by Eq. 7, as a function of evolution time for a 4-site lattice with disorder parameter \( W = 5 \) and Trotterization size \( \Delta t = 0.2 \). The “random” potential is fixed to be \( V(0, 1, 2, 3) = 0, 1, 3, 2 \), which may be computed with a single \( \text{CX} \) gate. The data points are obtained on physical quantum processors provided by IBM and Rigetti and are compared with the exact result. We perform 300 quantum measurements for each point to estimate \( D(t) \) and the stochastic errors shown are computed using bootstrap.

![Figure 5](image-url)  

**FIG. 5.** Circuit for evolving the link-disorder Hamiltonian of Eq. 8 on a three-qubit, eight-site system. For brevity, we use \( R_x = R_x(\theta \Delta t) \), and the increment and decrement circuits are not shown explicitly. Note that \( P \) and \( P' \) are independently sampled permutation matrices.
ACKNOWLEDGMENTS

We are grateful to Tom Cohen and Brian Swingle for their suggestions on the course of this work, and to Jay Sau for comments on an earlier version of this manuscript. A.A. is supported in part by the U.S. Department of Energy grant DE-FG02-95ER-40907. P.B. and S.L. are supported by the U.S. Department of Energy under Contract No. DE-FG02-93ER-40762.