Quantum states can be scrambled extremely quickly

The surprising theoretical result holds both good news and bad news for the ease of making quantum measurements.

FIGURE 1. THE RIFFLE SHUFFLE is an effective way to quickly scramble the order of a deck of cards. The number of shuffles you need to perform depends on how thoroughly you want the cards to be randomized. (Image by Johnny Blood/Wikimedia Commons/CC BY-SA 2.0.)

Randomness takes time. If you're playing a card game with a standard 52-card deck, shuffling the cards just once or twice isn't enough to mix them up. A quick-thinking and attentive opponent could make meaningful guesses about the cards' post-shuffling order.

For most card games played by humans, seven riffle shuffles (the type shown in figure 1) suffice to mix a standard deck. But it doesn't completely randomize the cards: Some of the 52! (about 8×10^{67}) possible orders are still significantly more probable than others. If a uniform likelihood over all possible orders is your goal, you need to keep shuffling much longer.

New theoretical work by Thomas Schuster, Hsin-Yuan Huang (both at Caltech), and Jonas Haferkamp (of Saarland University in Germany) highlights the enormous gap between "truly random" and "random enough for practical purposes" in the quantum realm. It was already known that for a randomly chosen quantum circuit to truly scramble an n-qubit state, the complexity of the circuit needs to grow exponentially with n: If the number of qubits is doubled, the number of layers in the circuit is squared. Like any exponentially growing function, it quickly becomes unwieldy for large inputs.

Schuster, Huang, and Haferkamp proved that one can achieve a sufficiently scrambled state with a much, much smaller circuit.[1] A practically random circuit, indistinguishable from an exponentially sized one, can be built with a number of layers that scales just logarithmically with n: Squaring the number of qubits merely doubles the number of layers.

Uniquely quantum

It's a surprising result, to the point where the researchers themselves struggled to believe it at first. To see how strange the quantum situation is, it's helpful to consider the analogous classical system, illustrated in figure 2a. As the problem is typically posed, the input bits are arranged in a single-file line, and each layer of the scrambling circuit contains logic gates that operate on adjacent inputs.

Given that setup, a circuit needs to have at least $n - 1$ layers to fully scramble an n-bit state, because that's how long it takes for the influence of the first input bit to propagate to the last output bit. A circuit with fewer than $n - 1$ layers could never have the same effect as one with more, and it could always be easily exposed by testing it with two input states that differ only in the value of the first bit. Most of the bits in the output would necessarily be the same in each case.

So why is the quantum situation different, to the point where a logarithmically sized circuit can, for practical purposes, scramble a state just as well as an exponentially large one can? One part of the answer hinges on what's meant by "for practical purposes": It means that the circuit can be tested no more than some fixed number of times k. The other part hinges on the nature of quantum measurements: Measuring a quantum state doesn't reveal everything about it—and much of the time, it reveals nothing.

"Imagine that a particle is in a state of fixed position, and you try to measure its momentum," says Schuster. "You get a completely random measurement outcome, and the information about the position is lost. In many-body quantum systems, there are exponentially many possible observables, and most of them don't commute with one another, just like position doesn't commute with momentum."

In other words, if you tried to perform the quantum equivalent of the classical experiment that's sketched in figure 2a, most of the time you'd be stymied by the fact that the circuit output probably isn't an eigenstate of whatever observable you chose to measure. Two similar inputs could produce similar outputs, but

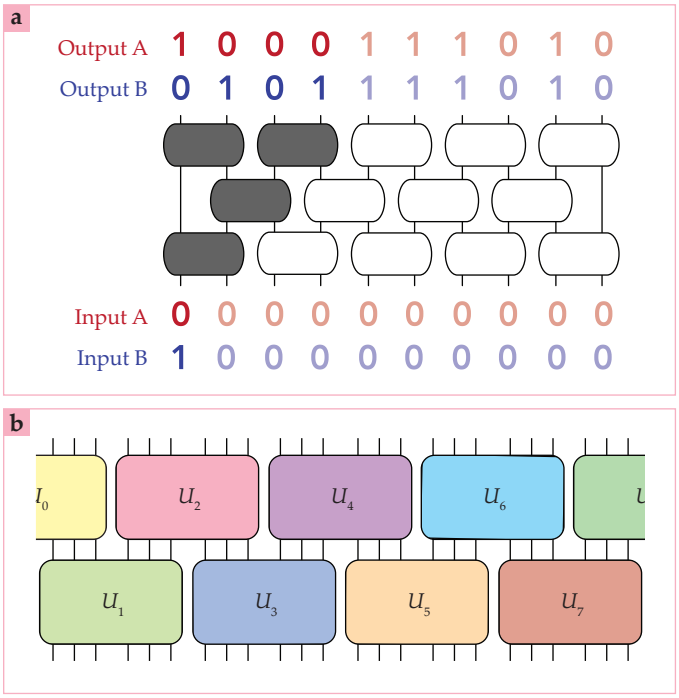

FIGURE 2. A CLASSICAL STATE (a) can't be thoroughly scrambled by a circuit with fewer layers than the number of input bits—at least not if the bits are arranged in 1D and the circuit gates operate on them locally—because, as the two test cases A and B illustrate, the influence of the first bit can't propagate all the way to the other end. But that argument doesn't apply to quantum states. An effectively random quantum circuit **(b)** can be built by grouping the qubits into small bunches and applying two layers of smaller scrambling circuits U_i, as shown. (Images adapted from ref. 1.)

you'd never know it unless you were lucky enough to guess the right way to probe the output states that wouldn't be affected by quantum measurement randomness. Most of your k chances to test the circuit are necessarily wasted, so even if k is large, it doesn't take a complicated circuit to make it look like the state is being completely scrambled.

But even with their expert intuition for quantum states and measurements, the researchers were surprised that so small a quantum circuit would be so effective. "Had you asked me two years ago whether this was possible, I would have emphatically said no," says Haferkamp. "Such a shallow circuit can't accumulate enough entanglement to approximate the near-maximal entanglement we thought we'd need. But that argument is flawed, because it turns out that near-maximal entanglement isn't something that can be detected in actual quantum experiments."

Not only did the researchers prove that a simple scrambling circuit is possible, but they also presented a formula for building it, as shown in figure 2b. Starting with n qubit inputs in a 1D line, they group the qubits into smaller bunches whose exact size depends logarithmically on n and k. They apply a randomly chosen scrambling circuit U to each bunch, then regroup the qubits and apply a second layer of scrambling circuits. Overall, the total number of layers in the circuit is logarithmic in n and k, and the researchers mathematically proved that, given the parameters of the test, the small circuit is indistinguishable from an exponentially large one.

Efficiency from randomness

"Our results contain both good and bad news," says Schuster. "We showed that quantum mechanics allows systems to hide information extremely rapidly. On the bad side, if a quantum state in nature or in the laboratory is hiding its properties from us, it becomes much harder for us to study. But if we ourselves are the ones hiding the information—and we know how it is hidden—it can be very useful."

Accordingly, the implications of the result include two broad classes of ideas: counterexamples and applications. The

counterexamples can be used to prove that there can be no way to efficiently detect certain quantum properties, such as quantum topological order, in systems that have been scrambled for even a short time, because a little scrambling is indistinguishable from a lot of scrambling.

On the other hand, applications of the result include ways to perform other types of quantum measurements more easily than was previously thought possible. It might seem strange that performing uncontrolled scrambling operations on a quantum state would be the key to understanding it. But a similar idea underlies Monte Carlo simulations in the classical realm, in which randomness is used to quickly sample a space of possibilities that's too large to study systematically.

Along those lines, in 2020, Huang and two other colleagues, Richard Kueng and John Preskill, conceived of a technique called classical shadow tomography, in which an observer can efficiently extract information about a quantum state by repeatedly applying random operations to it.[2] "The role of the random operation is to effectively rotate the quantum object," explains Huang, "so the classical observer can look at it from different angles."

Although the number of required rotations is small—it scales logarithmically with the amount of information the observer wants to extract—researchers previously thought that each one would take impractically long to implement. With the new insight that effectively the same randomizing operations can be applied much more quickly, classical shadow tomography becomes a potentially more practical technique.

The new work is theoretical, but the researchers note that there's no barrier to experimentally building the circuits they describe, because all the component quantum gates are already being used in labs in even greater numbers. "Shallow circuits are strictly easier to build than deep circuits," says Schuster. "In fact, it's likely that they've already been built in quantum experiments before our work—it's just that their power was not recognized."

Johanna Miller

References

1. T. Schuster, J. Haferkamp, H.-Y. Huang, *Science* **389**, 92 (2025).
2. H.-Y. Huang, R. Kueng, J. Preskill, *Nat. Phys.* **16**, 1050 (2020).

A machine that mechanically interlocks molecules

Researchers have shown how a molecular motor can be used to intertwine two molecules and form a linkage that couldn't be made with conventional synthesis.

It might be impossible to quantify the number of machines involved in daily life. We use machines to control the climate in our homes, move between places, and heat up water for our morning cup of coffee or tea, among other things. Somewhat less obvious, though, is the fact that our very ability to get up in the morning and make a caffeinated drink relies on a more hidden kind of machinery: molecular machines that convert the energy and carry the signals that power our bodies. Those tiny biological machines serve as inspiration for work that extends human engineering capacity down to the molecular level.

"The molecular scale, obviously, has very different rules than the macroscopic scale. Everything flies around in this Brownian hurricane all the time—everything moves and vibrates and

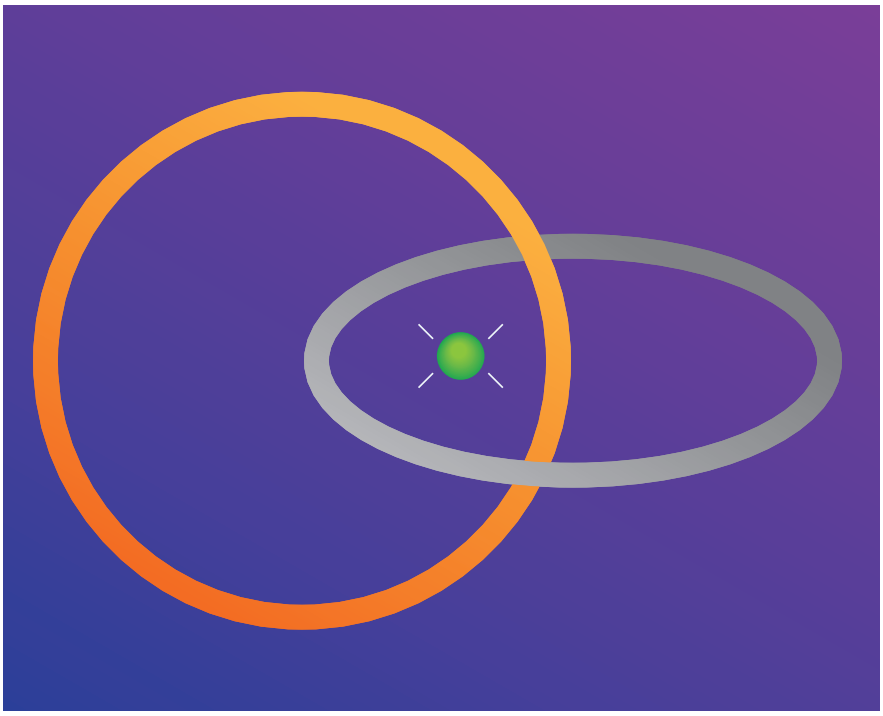

FIGURE 1. MECHANICALLY INTERLOCKED MOLECULES are connected not by chemical bonds but by their shapes, which makes them useful for engineering at the molecular scale. Ring-shaped molecules, represented here by orange and gray circles, can be connected like links in a chain to form what is known as a catenane. Catenanes have been effectively synthesized for decades by using ions, such as copper (green dot), that temporarily hold them in place—a process known as templated synthesis. (Illustration by Freddie Pagani.)