Mehau Kulyk/Science Photo Library

Can we exploit the weirdness of quantum mechanics?

Harnessing quantum entanglement will be the key to realizing large-scale quantum computers that solve hard problems, argues John Preskill

John Preskill is the Richard P Feynman Professor of Theoretical Physics at the California Institute of Technology, US, e-mail preskill@theory.caltech.edu, *Twitter* @preskill

Quantum theory is over a century old, yet physicists continue to be perplexed and delighted by the weirdness of the quantum world. Whereas the laws of classical physics successfully explain the phenomena we experience every day, atoms and other tiny objects obey quantum laws that sometimes seem to defy common sense, baffling our feeble human minds. In the 21st century, we hope to put this weirdness to work by building quantum computers capable of performing amazing tasks.

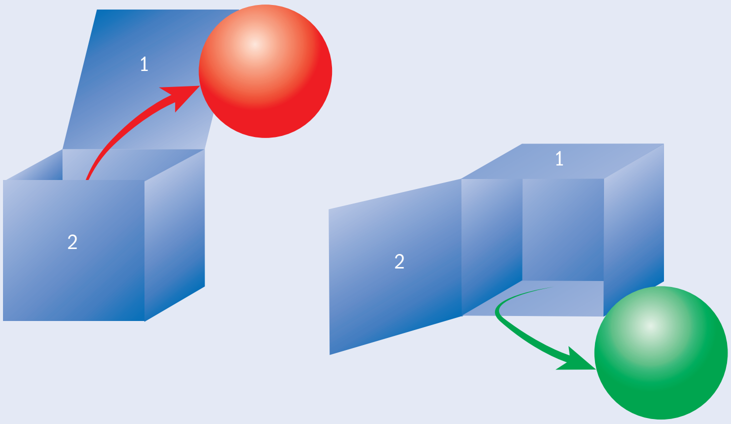
To appreciate how the classical and quantum worlds differ, it is helpful to recall how information gets encoded and processed by physical systems. Just as digital information can be expressed in terms of bits, information carried by quantum systems can be expressed in terms of indivisible units called quantum bits, or "qubits". A qubit is just a quantum system with two distinguishable states, and it can be realized physically in many possible ways; for example, by the spin of a single electron. But to get to the crux of how qubits differ from classical bits, let us view them more abstractly.

Boxing clever

We can picture a bit as a box with a ball inside that can be coloured either red or green. The box has a single door we can open to find out the ball's colour. A qubit is also such a box, but with two doors marked 1 and 2. Whenever we open the box, we must choose either door 1 or door 2; we cannot open both. However, opening a door not only reveals the colour inside but also unavoidably disturbs what is inside.

If we put a red ball in door 1 and later open door 2, the ball that comes out has a random colour: red with

Curious affair



A qubit can be viewed as a box containing a ball that is either red or green, the colour of which can be viewed by opening either of two doors (1 and 2). Strangely, we cannot predict what will happen when we observe the colour through, say, door 2, even though we know exactly how the box was prepared, for example, by opening door 1.

The technology for controlling quantum systems is advancing rapidly, fuelling the hope that in a few decades human civilization will enter an age of quantum supremacy

probability ½ and green with probability ½. Although we often use probability to describe classical systems, the randomness exhibited by quantum systems is different. If a classical box has a ball inside and we do not know the ball's colour with certainty, we assign probabilities to the two possible colours, reflecting our incomplete knowledge. But for the quantum box, we may be powerless to predict what will happen when we observe the colour through door 2, even though we have complete knowledge of how the box was prepared (for example, by opening door 1).

The deepest differences between classical and quantum information can be fully appreciated only if we consider systems with more than one part. So consider two qubits: Alice's in London and Bob's in New York. This qubit pair can be prepared in a state such that if Alice opens either door of her box in London she sees a random colour, and the same is true for Bob in New York. So neither party acquires any information by measuring his or her qubit. Instead, information is hidden in *correlations* between what Alice sees when she opens a door in London and what Bob sees when he opens a door in New York – in this particular state Alice and Bob are guaranteed to find the same colour if they both open the same door. There are four distinguishable ways in which boxes in London and New York could be perfectly correlated – Alice and Bob could see either the same colour or different colours when both open door 1 or both open door 2. By choosing one of those four ways, we have stored two bits in the boxes.

Classical systems can also be correlated, of course, but this is different. What's strange is that the information is completely inaccessible locally; it is entirely stored in the correlations. Though the whole system is in some definite state, the parts of the system are not. That is "quantum entanglement".

Stranger and stranger

Entanglement gets stranger still for systems with many parts. Picture a 100-page book. If the book were classical, then by reading one page we could learn 1% of the content of the book. But a highly entangled quantum book is different. Looking at any one page we see only random gibberish, learning almost nothing about the content of the book. That is because information does not reside on the individual pages; instead it is recorded in the correlations among the pages. Only by performing a complex collective observation on many pages at once can we discern the differences between one highly entangled book and another.

For a highly entangled state of a few hundred qubits, the correlations among the qubits are so complex that describing them completely using classical information would require an unthinkable number of bits – more in fact than the number of atoms in the visible universe. This extravagant complexity of the quantum world points toward a highly plausible but unproven conjecture: classical systems cannot in general simulate quantum systems efficiently. If true, this statement has extraordinary implications. It means that by building highly controllable, many-qubit quantum systems, we should be able to perform some information-processing tasks far faster than would be feasible if we lived in a classical – rather than a quantum – world.

The technology for controlling quantum systems is advancing rapidly, fuelling the hope that in a few decades human civilization will enter an age of quantum supremacy, in which quantum computers solve problems that are beyond the reach of classical digital computers, such as factoring large numbers and simulating the physics of complex molecules. But to realize that dream, we must overcome a formidable obstacle: that of "decoherence", which ordinarily makes large quantum systems behave classically. Entanglement among the qubits in a quantum computer is the source of its power, but entanglement between the computer and its unobserved environment is our enemy, driving decoherence.

In a classical computer an error occurs if interactions with the environment flip a bit. But a qubit is more delicate – it suffers an error if any information at all about its state leaks to the environment. That is decoherence. So for a quantum computer to work effectively, the information it processes must be perfectly concealed from the outside world until the computation is completed and the result is announced.

What weapon shall we wield to battle decoherence? Entanglement! The best way to resist decoherence is to encode information in highly entangled states. The state stored in the computer is like an entangled quantum book. The environment, interacting with the pages one at a time, acquires no information about the content of the book, because the information resides not in the individual pages but rather in the correlations among the pages. This principle, dubbed "quantum error correction", will guide the design of future quantum computing hardware and software.

Today's scientists and engineers are fortunate to live in an age of emerging quantum technologies. Indeed, our imaginations are poorly equipped to anticipate the many potential rewards to be gained by manipulating highly entangled quantum states. We should expect the unexpected. ■