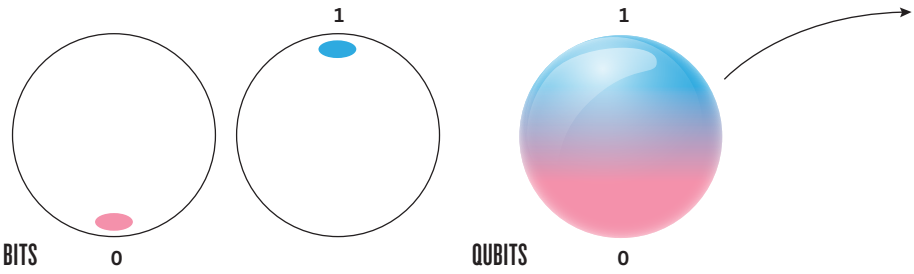
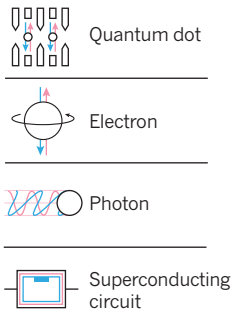
QUANTUM LEAPS, BIT BY BIT

The promises of quantum computation are unique — and so are the challenges. Progress in physics, mathematics, computer science and engineering have brought quantum computers to a point where they start to challenge their classical counterparts. By **Andreas Trabesinger**; *illustration by* **Visual Science**.

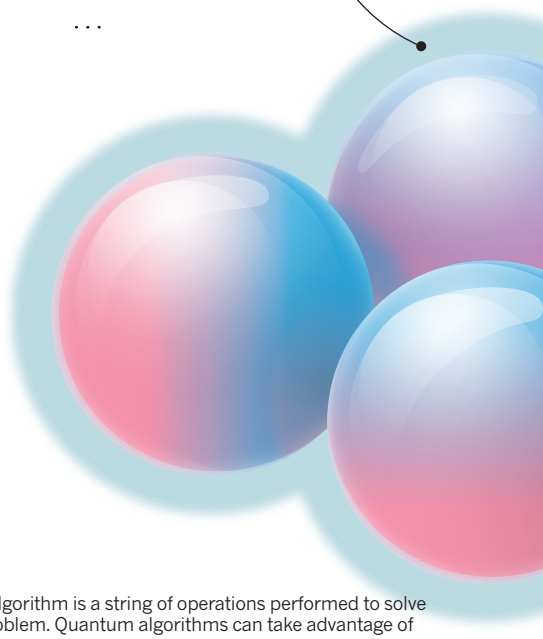
BITS VERSUS QUBITS

In classical computing, information is encoded in bits as a string of 1s and 0s. Ten bits gives 2^{10} or 1,024 combinations of 0s and 1s, which can represent one number between 0 and 1,023. By contrast, a qubit can represent both 0 and 1 at the same time (superposition), so 10 qubits can encode all 1,024 numbers simultaneously. Qubits can be created from several physical systems with distinct quantum states. Manipulate these systems using lasers or microwaves and it is possible to create quantum superpositions of the two or more states. Join many qubits together and a huge amount of information can be encoded.



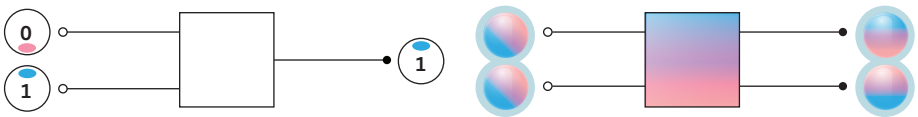


ENTANGLEMENT



PERFORMING OPERATIONS

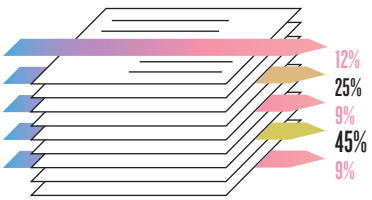
A classical computer operates on single bits, deriving an outcome that is either a 1 or 0. By contrast, a quantum computer takes the entire superposition state of all the qubits and transforms it into another superposition state that still encodes all numbers. During these operations the quantum system has to be protected against perturbance to avoid unwanted changes to the quantum state, which lead to errors or loss of quantum superposition.



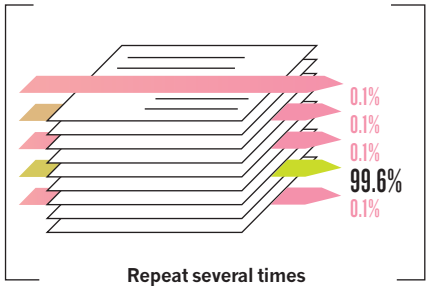
CLASSICAL Logic gate

QUANTUM Quantum logic gate

ALGORITHMS

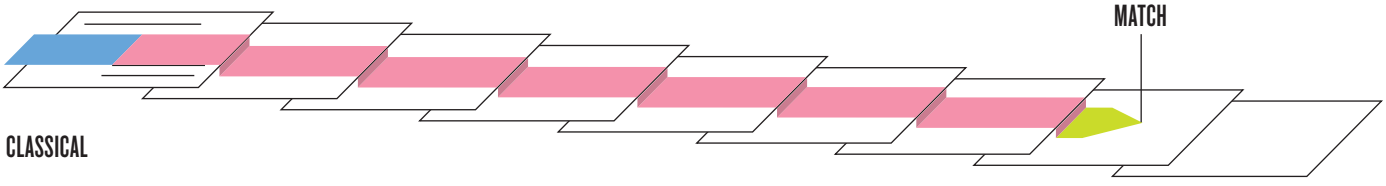


QUANTUM



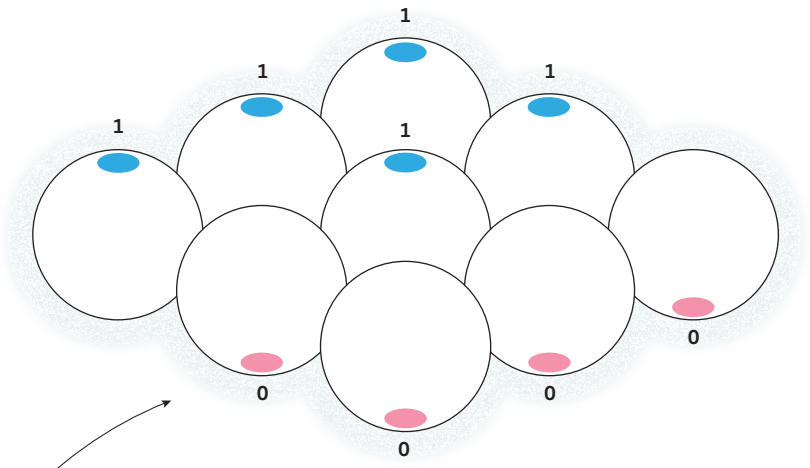
Repeat several times

An algorithm is a string of operations performed to solve a problem. Quantum algorithms can take advantage of the parallelism afforded by the superposition of states. This means that all possibilities are analysed at the same time, instead of individually — analogous to being able to scan all your business cards at once to look for a name. The quantum algorithm (known as Grover's algorithm) gives each card a probability of being 'right'. After several iterations, the cumulative probability of the target card will be higher than the others. Even if the algorithm has to be run several times, it is much quicker than classical searching. And the larger the database, the bigger the advantage.



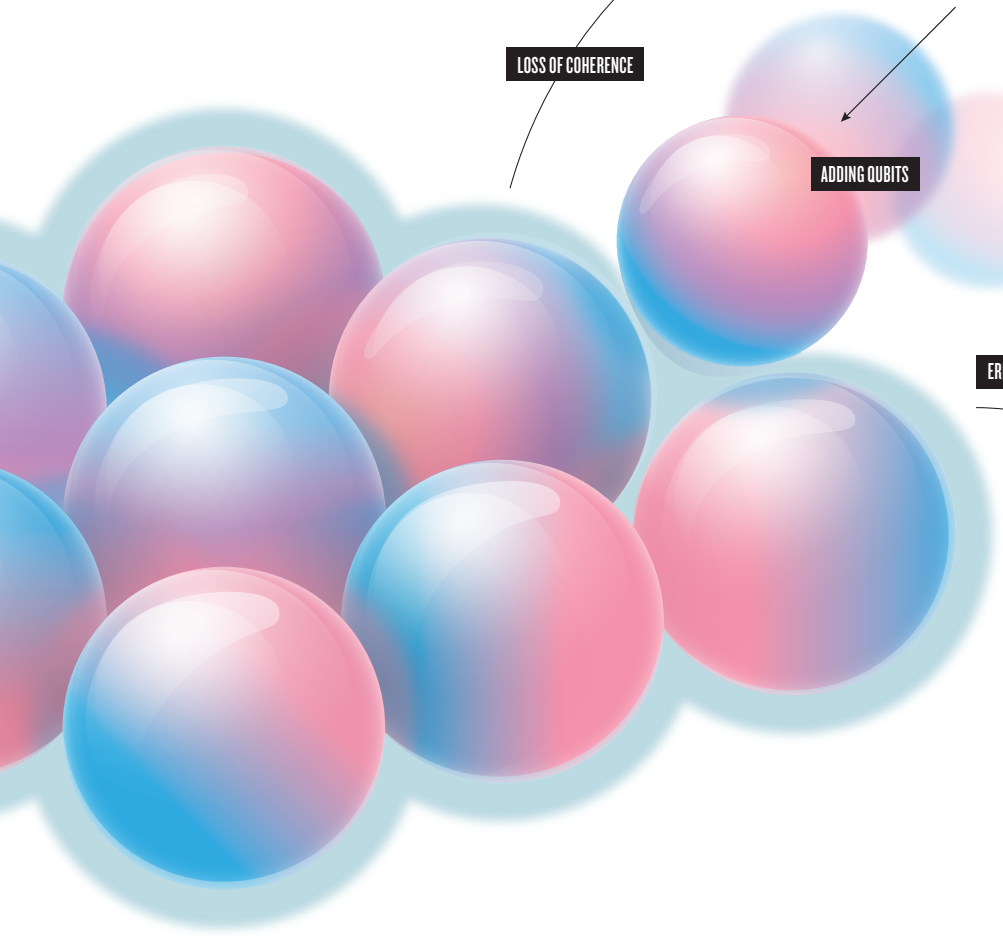
SMALL ELEMENTS, BIG CHALLENGES

Important challenges need to be addressed on the route to a large-scale quantum computer.



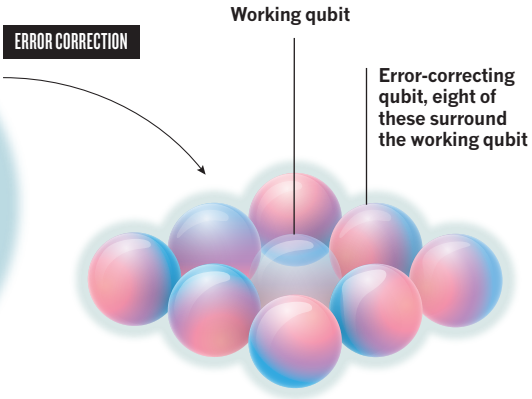
1 LOSS OF COHERENCE

Superposition enables quantum computers to process a lot of data in parallel, but maintaining coherent superposition of quantum states is challenging. Disturbances from outside destroy coherence. At the same time, qubits need to be controlled to perform operations.



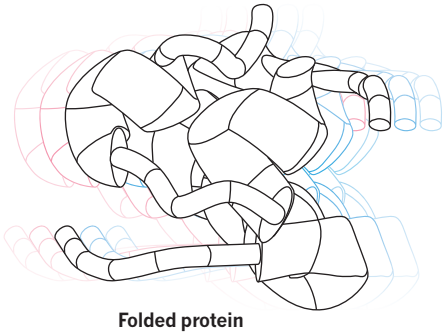
2 ADDING QUBITS

Each additional qubit must be able to enter into a state of superposition with the other qubits. Such particles are 'entangled', which means that they can influence each other in ways that classical particles cannot. More qubits make the overall quantum state more fragile. Scaling up a quantum computer quickly becomes a challenging juggling act.



3 ERROR CORRECTION

Classical computers have good error control, which enables robust outcomes despite imperfect components. To give quantum computers a similar level of fault tolerance and the capability to correct errors requires fresh approaches — typically adding ancillary qubits, making scaling up even more difficult.



Folded protein

ILLUSTRATION BY VISUAL-SCIENCE.COM

GAME CHANGERS: THE FUTURE

Quantum computing will not replace classical computing, but it will excel at tasks that are too complex for current computers, such as searching through huge databases or finding prime factors of large numbers. The latter is so hard that it forms the basis of encryption, which protects online activities. Using Shor's algorithm, a quantum computer might take weeks to find factors that would take state-of-the-art classical computers thousands of years. Quantum states can also be used for more-secure communication schemes. One application of quantum computers is to calculate the behaviour of other quantum systems. For example, quantum computing could be used to fully understand the chemistry of molecules, which requires knowledge of the quantum mechanics of their electrons, or to find the optimal configuration of a folded protein, for which there are vast numbers of arrangements. Classical computers can calculate the behaviour of quantum systems of about 50 qubits. When quantum computers with more than 50 usable qubits become available, they are set to establish 'quantum supremacy'.