Delicate information

Quantum computing

Is this the birth of a new technology for number-crunching, or is quantum information something more profound?

Rainer Blatt

Living in the 'information age', we are constantly concerned with a faster flow of information, made possible by the Internet, high-speed processors and communication links. 'Processor speed', 'memory capacity' and 'bandwidth' are terms that are known to us all, and our need for more of them drives one of the world's most flourishing industries.

Industry has long since described the rate of at which technology progresses in terms of a rule of thumb — commonly known as Moore's law — which simply states that processor speed, and hence computational power, doubles roughly every 18 months. This empirical law has proved to be valid over the past three decades and still holds today. It will not be long, therefore, before the number of atoms used to store a single bit of information becomes so small that the storage and processing of information will need to be described in terms of quantum mechanics. Eventually, a single atom will suffice for storing the information of a single bit, a state of affairs that will usher in the age of quantum computing.

With a single atom, information is stored in its quantum states, which can represent not only 0 and 1, but also otherwise rarely obtained 'superposition' states. In other words, the information may be found to be simultaneously 0 and 1, and a (quantum) measurement assigns it to either one of these states with a certain probability. This elementary type of information storage — termed a quantum bit or 'qubit' — seems to be an odd proposition, because at first it seems impossible to handle and process such elusive quantum information in a predictable way. Therefore, in the 1980s and the early 1990s, qubits and quantum information processing were considered to be a mere curiosity in the information sciences.

This point of view was shattered when Peter Shor of AT&T came up with a stunning algorithm in 1994. He showed that the factorization of large numbers — an extremely difficult and time-consuming problem for classical computers — can be achieved in a highly efficient, rapid way using a quantum computer. Large numbers and their prime factors are commonly used to encrypt data and messages, as it takes too long to factorize a large number — and thus decode the information — on a classical computer. If the factorization problem could be solved, then all current cryptographic systems would be seriously endangered. Peter Shor's result therefore spawned a worldwide attempt to create a real quantum computer, which could be applied to basic research and technology.

After more than five years of research, the field of quantum information is now thoroughly established, and earnest investigations are being made of about ten different technologies that may become the computing techniques of tomorrow. Is this the beginning of a new computer age — the birth of a new technology for number-crunching? Or is quantum information something more profound — perhaps a completely new concept — that is intellectually worth increased research efforts?

Although quantum computation is often hailed as the computing technology for the twenty-first century, it has become clear in recent years that today's computers will not be replaced by quantum counterparts. Aside from factorization, only a few algorithms run faster on a quantum computer, and the classical workhorses of information processing are set to remain in place for the foreseeable future. That favourite question of journalists — "when can I buy a quantum computer?" — is definitely beside the point here.

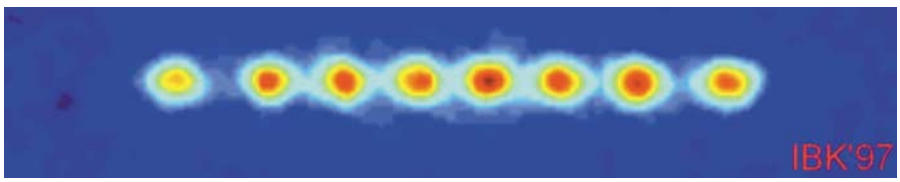
At best, current quantum technology can provide a system with a few (less than ten) qubits and a limited number of the processing operations that are required for computation. But progress over the past few years offers real hope that we will eventually be able to control and manage the technology to build and operate larger-scale quantum computers with a high degree of reliability. Comparatively speaking, however, at present we are not yet even at the stage of the ENIAC (electronic numerical integrator and computer), the 1940s predecessor of modern computers.

Nevertheless, viewing the fundamental physical laws of quantum mechanics from the angle of quantum information has had a remarkable impact so far. Five years ago, the ingredients of quantum computing technology were seriously thought to be uncontrollable. Handling and processing quantum information — that is, controlling the superposition states for extended periods of time and over ever-increasing distances — still requires very delicate procedures. Every unwanted interaction of a quantum storage device, such as an atom with its surrounding environment, would constitute a measurement and would thus lead to irretrievable loss of that information.

Nevertheless, research has shown that correction of errors at the quantum level is a genuine possibility, and can be used to protect and even to restore quantum information. This is a surprising and revolutionary result that was not foreseen even as recently as a few years ago. Aside from its potential technical impact, it clearly demonstrates the power of viewing fundamental physics with the information-guided eye. Quantum computation, and more generally, quantum methods for information processing and communication, not only provide new tools for the information age, but also represent one of the most powerful concepts since the discovery of quantum mechanics itself.

The schemes and techniques being investigated today will be the fundamental building blocks for tomorrow's general quantum technology. Thus, the control and measurement of large-scale quantum systems — what will come to be termed 'quantum engineering' — may be the key technology of the twenty-first century. ■

Rainer Blatt is at the Institute for Experimental Physics, University of Innsbruck, Technikerstrasse 25, A-6020 Innsbruck, Austria.



F. SCHMIDT-KALER & R. BLATT

Counting qubits: a string of ions representing a 'quantum byte' in an ion-trap quantum computer. Here all are in state '0'; exciting any one would cause loss of fluorescence at the corresponding position.

FURTHER READING

Bouwmeester, D., Ekert, A. & Zeilinger, A. (eds) *The Physics of Quantum Information* (Springer, Berlin, 2000).

Steane, A. *Rep. Prog. Phys.* **61**, 117–173 (1998).

Bennett, C. H. & DiVincenzo, D. P. *Nature* **404**, 247–275 (2000).