Quantum leaps in small steps

TOMMASO CALARCO[1]*, PHILIPPE GRANGIER[2], ANDREAS WALLRAFF[3] AND PETER ZOLLER[4]

are at [1]the Institute for Quantum Information Processing, University of Ulm, D-89069 Ulm, Germany; [2]the Institut d'Optique, Campus Polytechnique, RD128, F-91127 Palaiseau, France; [3]the Department of Physics, ETH Zurich, CH-8093 Zurich, Switzerland; and [4]the Institute for Quantum Optics and Quantum Information of the Austrian Academy of Sciences, A-6020 Innsbruck, Austria.

***e-mail: tommaso.calarco@uni-ulm.de**

Only long-term commitment can ensure that quantum information science eventually fulfils its promise of revolutionizing information-based societies.

The history of quantum mechanics is a history of revolutions. Scientifically, its discovery represented a radical paradigm shift with respect to contemporary physical theories. Technologically, its applications deeply affected everyday life. Some of the most far-reaching applications — such as the transistor and the laser — are the building blocks of current electronics and telecommunications, and have heralded the birth of information society as we know it today. Yet, they merely act as a support for a completely classical mode of processing information, where logical degrees of freedom exhibit no quantum behaviour whatsoever. The realization of this fact led at the beginning of the 1980s to speculations, initiated by Richard Feynman, about the possible use of quantum-physical systems to perform calculations of complexity unattainable by systems behaving classically[1]. Around that time, coming from a completely different corner, several researchers were already investigating fundamentally counterintuitive aspects of the theory, like the superposition principle exemplified in the Schrödinger cat paradox[2] and the 'spooky action at a distance' resulting from quantum entanglement[3].

FROM PARADOX TO TECHNOLOGY

Two theoretical breakthroughs turned these first, rather foundational inquiries into application-oriented research: the quantum key distribution (QKD) protocol[4] of Gilles Brassard and Charles Bennett, presented in 1984, and Peter Shor's quantum factorization algorithm[5] from 1994. Shor's algorithm is a method for decomposing a number into prime factors in a time exponentially shorter than any known classical algorithm would take and, as such, provides a possible route to breaking many of the currently used cryptographic codes. The 'BB84' QKD protocol, on the other hand, provides — somewhat ironically — a way to transmit a secret message with absolute security, even against eavesdropping attacks carried out with a quantum computer.

Both methods rely essentially on the ability to preserve and coherently manipulate superpositions of quantum states. This is relatively easy to achieve for quantum information encoded in photons propagating in free space or in optical fibres. Therefore, QKD — popularized as 'quantum cryptography' — has been developing quite successfully in recent years. But ultimately, for large bit rates or large distances (that is, more than about 100 km), noise and loss in photonic channels prevent secret bit transmission in practice. This limitation was lifted, in theory, about 10 years ago by introducing 'quantum repeaters'. These are, in essence, error-correcting devices that counteract the effect of the 'environment' on the qubits (such perturbations are unavoidable because no quantum system can be completely isolated from its surroundings). In the more general context of quantum computation, quantum error-correction codes[6] — invented in 1993 by Shor and Robert Calderbank, and by Andrew Steane — theoretically allow for arbitrary quantum computations to be performed even with faulty gate operations, provided the error probability per gate is sufficiently small.

A TIMELINE FOR FEASIBILITY?

Solutions do exist then, on paper, to reach the ultimate goals — that is, unconditionally secure communication and devices that deliver immense computational power. But what about implementation? A crucial constraint, which doesn't come as a big surprise, is that arbitrarily scaling up the number of qubits in a quantum computer, or the distance covered by a quantum communication channel, requires that the initial 'uncorrected' error rates are already quite small. Unfortunately, the required values are not yet attainable practically. Several schemes for high-quality quantum gates have been put forward, starting with the ion-trap quantum computer proposed in 1995 by Ignacio Cirac and Peter Zoller[7]. An increasing number of groups are trying to implement quantum gates with experimental systems as diverse as ultracold atoms, Josephson junctions and quantum dots. Still, no one has yet reached the fault-tolerance threshold for a two-qubit gate, or realized a working quantum repeater.

To get a clearer view of the challenges that have to be overcome on the way to practical quantum information processing (QIP), 'roadmaps' have been put in place on both sides of the Atlantic. The US version, last updated by the Department of Defense's Advanced Research and Development Activity (now called Disruptive Technology Office) in 2004, prescribed quantitative goals, and defined measures of the progress in each subfield. The first deadline — for achieving repetitive error correction on ten qubits by 2007 — has already been missed. The European 'Quantum Information Processing and Communication Strategic Report'[8], supported by the European Commission's Future and Emerging Technologies Unit and maintained by a panel of scientists, has a less rigid approach, but still sets ambitious long-term goals that will require substantial progress to be made.

Though there is clearly a long way to go, recent successes justify an optimistic outlook on the future of QIP, not least in the face of the high expectations for applications that become possible once the technology has matured. The pace with which progress has been made, on both the theoretical and the experimental side, could not have been envisioned ten years ago. Controlled

interactions and entanglement — required for scalable quantum computing — have been demonstrated with a number of physical systems, from trapped ions and atoms in optical lattices to quantum dots and superconducting circuits. Some earlier platforms, like NMR, are fading away in view of their limited scalability, but new ones keep emerging, both experimentally (for example, colour centres in crystals) and theoretically (for example, polar molecules). Also, mathematical proofs have been given for the security of various quantum communication protocols, new efficient quantum algorithms have been found and alternative computer paradigms have been proposed. In short, by advancing towards 'scalability', QIP has overcome all of the first obstacles along its way towards practical working devices.

It is also safe to say that no ultimate roadblocks are in sight for QIP — in contrast to the 'classical' International Technology Roadmap for Semiconductors (ITRS), which will sooner or later hit the atomic scale. However, setting a precise timeline may be not so useful in a field that, after all, is still in its infancy; the ITRS was established only in 1994, more than fifty years after the invention of the transistor. A much more effective way to picture where the field is going might be to look at the most important recent results. A comprehensive overview is given in the European report mentioned above[8]. Here, we pick the main results from the last two to three years, based partly on our subjective appraisal and partly on the selection underlying the program of a recent Gordon conference[9].

RECENT ACHIEVEMENTS

Most platforms for QIP fall roughly into two major categories: atomic, molecular and optical (AMO) systems and solid-state systems. In the first category, a qubit can be encoded, for instance, in two internal states of a trapped atom or ion, cooled to its vibrational ground state. Single-qubit operations are effected by laser-induced Rabi rotations, and two-qubit gates can be accomplished by exploiting a variety of 'quantum bus' coupling mechanisms (via cavity photons or common-mode ion-trap phonons) and controlled interactions (from collisions to dipole–dipole interactions between Rydberg-excited atoms, to electrostatic forces between ions). The brightest candidates so far are trapped ions, and atoms confined in optical lattices. Systems based on trapped ions lead the race with respect to controlling individually a few qubits (up to eight qubits, a 'quantum byte'), whereas atoms in optical lattices provide a very large number of qubits in parallel, amenable to pair-wise interactions; combining this high parallelism with individual addressability is the next challenge. There are many other contenders, including photons within the 'linear quantum computing' approach[6], miniature traps for atoms or ions (known as atom chips or ion chips), as well as 'continuous variables' systems, where the usual qubit-based approach is replaced by continuous degrees of freedom, such as the amplitude of the quantized electric field, or collective spin in atomic ensembles.

The past three years have also seen impressive progress in the development of solid-state architectures for QIP. Information can now be stored and manipulated routinely in single charge, flux or spin degrees of freedom that are realized controllably in super- or semiconductor micro- and nanoelectronic circuits. Careful device design and choice of materials have pushed single-qubit coherence times into the microsecond range. Accurate qubit control on nanosecond timescales and high-fidelity qubit read-out using 'quantum non-demolition schemes' have been instrumental for the demonstration of controllable two-qubit coupling, and the first realizations of two-qubit gates in a number of different architectures. Inspired by atomic physics and quantum optics, cavity quantum electrodynamics ideas are now harnessed in solid-state systems to realize controllable coherent coupling between electronic qubits and individual photons. This approach is promising for implementing non-local qubit coupling schemes that are important in truly scalable architectures and as an interface for novel hybrid QIP systems. The next major challenges in solid-state QIP include the realization of high-fidelity control of multi-qubit systems, the full characterization of multi-qubit dynamics by process tomography and also the continued effort to further improve coherence times through materials research.

On the theoretical side, in addition to the 'standard' concept of a general-purpose quantum computer capable of performing quantum algorithms such as searching databases or factorizing numbers, renewed attention is being paid to Feynman's original idea of a quantum simulator: hamiltonian models, like Hubbard's, that are relevant for a range of physical phenomena, from antiferromagnetic materials to *d*-wave superconductors, can be made tractable by encoding them in a different physical system, from atoms in optical lattices to trapped-ion crystals.

Within the vast range of QIP activities, quantum communications and especially quantum cryptography are currently the most advanced ones, as far as applications are concerned. Several small companies worldwide are now selling QKD devices that yield decent data rates over distances of several tens of kilometres, and many large companies with an interest in telecommunication or information technology sustain an internal research program on the subject. Furthermore, much has been done regarding a fair assessment of advantages and disadvantages of different approaches — this is probably the best way to convince potential customers. A useful document is the 'White Paper on Quantum Key Distribution and Cryptography'[10], issued by the European integrated project for the development of a global network for secure communication based on quantum cryptography (SECOQC).

A major challenge for quantum communications is the construction of a practical quantum repeater; such a device would be very useful for quantum communications *per se*, but would also be a significant advance towards quantum computing. Clearly much remains to be done, but first steps have been made, for instance by using single-photon emission and storage within atomic ensembles[11], or in general towards quantum memories, which are required for a fully operational quantum network.

To conclude, although there is no 'working quantum computer' yet, within the past ten years quantum information science has already advanced quite a long way towards its objectives. The major issues are well-identified, and there is a general consensus about the most important achievements so far, and the ways that should be taken. Overall, research is progressing and becoming increasingly focused, with no signs of stagnation. Maybe the most difficult aspect to explain to outsiders — and 'deciders' — is that coping with the laws of nature has never been easy. Every step takes serious effort. And therefore, only long-term commitment can be successful.

References

1. Feynman, R. P. *Int. J. Theor. Phys.* **21,** 467–488 (1982).
2. Schrödinger, E. *Naturwissenschaften* **23,** 807–812; 823–828; 844–849 (1935).
3. Aspect, A., Dalibard, J. & Roger, G. *Phys. Rev. Lett.* **49,** 1804–1807 (1982).
4. Bennett, C. H. & Brassard, G. in *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing* 175–179 (IEEE, New York, 1984).
5. Shor, P. W. in *Proc. 35th Ann. Symp. Foundations of Computer Science* (ed. Goldwasser, S.) 124–134 (IEEE Computer Society Press, New York, 1994).
6. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge Univ. Press, 2000).
7. Cirac J. I. & Zoller, P. *Phys. Rev. Lett.* **74,** 4091–4094 (1995).
8. QIPC Strategic Report 2007; available via http://tinyurl.com/2svz5y.
9. Gordon Research Conference on Quantum Information Science (15–20 April 2007, Lucca, Italy); available via http://tinyurl.com/23933h.
10. SECOQC White Paper on Quantum Key Distribution and Cryptography (22 January 2007); available via http://tinyurl.com/2k97tz.
11. Duan, L.-M., Lukin, M. D., Cirac, J. I. & Zoller, P. *Nature* **414,** 413–418 (2001).