A quantum leap in computing power

Tommaso Calarco, from the University of Ulm, Institute for Quantum Information Processing, on the future of high speed computing…

Quantum physics is a child of the first decades of the 20th Century. It has led to numerous groundbreaking applications, including, for example, the laser, the understanding of semiconductors and thus of modern computer technology, and many more. Whilst offering all these technological advances, quantum physics has been, from the very beginning, linked to fundamental questions about how nature really works. Such questions have triggered fundamental experiments, demonstrating that the world is not as simple as early physicists had hoped but is really as strange as quantum physics suggests, revealing the 'reality' of counterintuitive concepts such as quantum superposition, the ability of a particle to be in two places at once, and quantum entanglement, a direct connection between distant particles that Einstein called 'spooky'. To the surprise of many of the early participants of these experiments, the resulting deeper understanding of the fundamental laws of the quantum world, in combination with the theory of information and computer science, opened up an avenue for a new information technology, Quantum Information Processing and Communication (QIPC).

QIPC is based on the control and manipulation of quantum entanglement and superposition for the purpose of encoding, processing, transmitting and decoding information. It holds the promise of immense computing power beyond the capabilities of any classical computer. Quantum communication offers means to securely transmit secret information through various methods of quantum cryptography, or to even teleport the quantum state of a physical system, which offers a novel way of communication between and within future quantum computers. QIPC is also directly linked to emerging quantum technologies such as quantum-based metrology and sensing.

The important challenges of quantum computing and quantum communication in the immediate future have been identified in the European QIPC Strategic Report[1]. They include further development of quantum computer implementations beyond the present proof of concept demonstrations. Specifically, present demonstrations can only handle a limited amount of quantum information bits (qubits), currently well below 10, and are still sensitive to environmental influences such as electromagnetic fields, polarisation fluctuations in optical fibres and others, which prevent the exploitation of the full potential of quantum computers. The objectives of current research efforts therefore involve the development of devices that can realise quantum algorithms with up to 10 qubits and that show a clear perspective to be scalable to multiples of tens of qubits. Along with scalability, an additional focus is on the demonstration of fault tolerant computing and error correction, both by improving current approaches and by developing new fault tolerant architectures. Another approach to overcome current limitations is to devise and implement distributed quantum algorithms that would operate on networked elementary quantum processors.

A challenge specific to the realm of quantum communication is the implementation of real world quantum networking. This requires the ability to distribute quantum information efficiently over large distances and to store quantum information over long times. At present, distributed entanglement has been shown up to hundreds of kilometres by using entangled photons, and storage of quantum information has been shown up to tens of seconds. A next step has to bring these techniques together. Current developments in quantum communication therefore focus on the interfacing of different quantum systems, in particular photons with matter, to interface qubit memories and carriers of quantum information. To distribute quantum entanglement over even larger distances will require so-called quantum repeaters that teleport entanglement between several nodes or the use of satellites that distribute entangled photons via optical links. Finally, a working quantum network should demonstrate secure quantum key distribution between quantum links connecting multiple distant nodes.

A further challenge presently faced is that of bringing QIPC one step closer to commercial exploitation of Quantum Information Technologies (QIT), ie. technologies that represent genuine applications of QIPC (eg. quantum metrology, quantum sensing, quantum imaging, quantum random number generators), or technologies that are instrumental in developing QIPC devices (eg. single and entangled photon sources and detectors, chips for ion and atom traps). In order to encompass the full range of quantum information from conception to development of devices, integration of the scientific base is required, from computation and communication, to other technological applications of quantum entanglement and superposition.

These efforts will eventually lead to a pool of reliable technologies for the different components of a quantum architecture, much like it had happened for classical computers where magnetic, optical and electric bits are now used for storage, transmission and processing of information, respectively. All of these goals are, of course, to be considered both experimental and theoretical: Aside from finding and investigating fundamentally new algorithms and protocols for QIPC, theory must in fact guide and support experimental developments, covering a wide range of physical systems and technologies.

The development of the field is presently driven by many research groups worldwide, with Europe taking the lead in a significant number of activities. Besides these worldwide research activities, a technological reason for expecting QIPC to be the core of future information technology is the mere fact that devices become smaller and smaller, which implies that on a timescale of about 20 years, a situation will be reached where one bit of information is carried by a single electron or atom, even in existing computers. Likewise, in communication technology, a clear development is to use less and less light energy to encode and transmit a single bit. Quantum information processing is likely to emerge as a natural consequence of this development. It is interesting to note that the expectation of when QIPC will be a mature technology and the expectation of when classical computers will reach their limit lead to similar timescales.

As has often happened in the history of science, fundamental questions have once more led to ideas for a new technology. Yet, as again often observed in the history of technology, the resulting technological progress has led to new fundamental questions. Because of the multi-disciplinary nature of QIPC, with scientists coming from theoretical and experimental physics, computer science, mathematics, material science and engineering, these new questions emerge along several directions. For example, new computational methods born within QIPC will allow solving problems ranging from many-body physics to quantum field theory, while QIPC enabled quantum simulations will provide the possibility to model new materials in a superior way. Also, entangled state engineering will push the metrology and sensing towards and beyond quantum limits of sensitivity, hence enabling a completely new generation of high precision experiments that allow testing quantum predictions with unachieved accuracy. Other questions include the relevance of fundamental concepts such as realism, non-locality or information for an understanding of quantum theory, but also the possibility to prepare quantum superpositions and entanglement of increasingly large and massive systems such as molecules, atomic ensembles or even mechanical levers, which is deeply connected to the question about how the classical world emerges from the quantum one.

This way of connecting the most fundamental theory with fundamental experimentation in the quantum world, whilst at the same time offering novel, practical and revolutionary applications relevant for information and communication technology, is what sets QIPC apart from most other fields of science and technology, and that makes it so desirable and interesting, but at the same time so challenging and evasive.

[1] Available at http://www.qurope.net/Q_Reports/q_reports.php?type=reports&trig_id=1.

Professor Tommaso Calarco
University of Ulm
Institute for Quantum Information Processing
Tel: +49 731 5022832
tommaso.calarco@uni-ulm.de
www.uni-ulm.de

Dr Markus Aspelmeyer
Institute for Quantum Optics and Quantum Information (IQOQI)
Austrian Academy of Sciences
Vienna
Austria
Tel: +43 1 4277 29574
markus.aspelmeyer@quantum.at
www.iqoqi.at

Dr Daniele Binosi
European Centre for Theoretical Studies in Nuclear Physics
Italy
Tel: +39 (0461) 314 730/738
binosi@ect.it
http://qist.ect.it

Professor Rainer Blatt
Institute for Experimental Physics
Innsbruck University
Institute for Quantum Optics and Quantum Information
Austria
Tel: +43 512 507 6350
Fax: +43-512-507 2952
Rainer.Blatt@uibk.ac.at
www.iqoqi.at

Professor Anton Zeilinger
University of Vienna
Institute for Quantum Optics and Quantum Information(iqoqi)
Tel: +43 (0)1 4277 51201
zeilinger-office@univie.ac.at
www.quantum.at/zeilinger
www.iqoqi.at

Professor Eugene Polzik
The Niels Bohr Institute
Copenhagen University
Tel: +45 35 32 52 09
Fax: +45 35 32 50 16
polzik@nbi.dk
www2.nbi.ku.dk/side46811.htm