THE QUANTUM REVOLUTION - TOWARDS A NEW GENERATION OF SUPERCOMPUTERS -

R. BLATT

Institut für Experimentalphysik, Universität Innsbruck,
Technikerstr. 25, A-6020 Innsbruck, Austria, and
Institut für Quantenoptik und Quanteninformation (IQOQI),
Österreichische Akademie der Wissenschaften,
Otto-Hittmair-Platz 1, A-6020 Innsbruck, Austria

Computers that operate with quantum processes promise unprecedented computational power for some algorithms, much more than could be obtained by classical machines. The implementation of such a quantum computer requires the precise control and manipulation of individual quantum systems, a task that can be achieved by quantum optical means and the use of precision laser spectroscopy.

Keywords: Quantum computing, entanglement, trapped ions

1. Introduction

Computing machines have always been a dream of mankind and many mechanical tools have been developed to allow for faster and more complicated calculations. While the tools of the 19th century were mostly of mechanical nature, the technical evolution of the 20th century allowed the construction of fast electronic switches and hence the development of powerful computing machines. This led eventually to the revolution of technology by the ubiquitous availability of personal computers and its corresponding use in all areas of our daily life.

2. Computers and technology

The technical advance in computer technology is well illustrated by Moore's law[1] that states that nowadays computing power, as indicated by the number of transistors in a processor or the available memory on a chip, doubles approximately every 24 months. Surprisingly enough, this empirical law holds since more than 40 years and provides a guideline for the manufacturing industries. Also, the number of atoms that are required, for example, to store the information of one bit, decreases in a similar way.[2] While the storage of a single bit required about 10^{18} atoms in 1962, only 10^{10} atoms were necessary in 1988 and this trends still holds. Assuming an ongoing development, a simple extrapolation reveals that around 2020 only a single atom would carry the information of one bit. Clearly, at this stage the laws of quantum mechanics will govern the storing and retrieving of information; in practice, however, quantum mechanical effects will become important a long time before that.

Therefore, it seems natural to investigate whether using quantum physics for information processing can actually be used to our advantage. Already in the 1980s Deutsch and Feynman have discussed information processing using quantum physics,[3,4] however, at that time this subject was more an academic exercise since it was neither known how quantum information processing could be particularly useful nor how it could be implemented.

This situation changed in 1994 when Peter Shor came up with an algorithm[5] to factor large numbers that required only polynomial efforts (in terms of the digits of the number in question) while a classical computer needs an exponential overhead to solve this problem. This application, which is of enormous impact for cryptology, and the later found fast data base search by Lov Grover[6] led to an intense search for physical systems that allow one to really implement quantum computing. Thus, the mid 1990s mark the start of the quest for a quantum computer that is still ongoing and inspiring wide fields in physics today. Meanwhile, quantum information processing has matured as a multidisciplinary area in physics and computer science that ranges nowadays from most fundamental theoretical concepts to implementations using technologies from laser physics and laser spectroscopy to solid state and condensed matter physics and the field is still growing and widening.

3. Quantum bits, registers and gate operations

The smallest unit of classical information is the bit, usually represented by a switch either in "up"/"down" or "0"/"1" position. More generally, the quantum system comprised of the two levels $|0\rangle$ and $|1\rangle$ can be written also as the superposition

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \tag{1}$$

and this two-level system is commonly known as a quantum bit, or short, qubit. While a classical bit is best visualized as a switch, the qubit must be described as an arrow pointing somewhere on the surface of a sphere as is indicated in Fig. 1. For a quantum register, a row of several qubits is

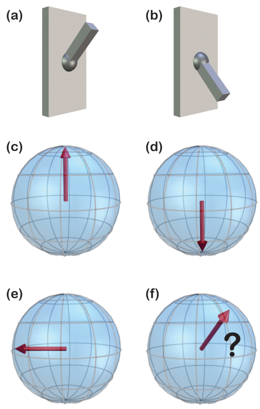

Fig. 1. Classical information (a,b) and quantum information (c-f). (c,d) show the system in state $|0\rangle$, $|1\rangle$ respectively, (e) describes a superposition of equal weights $|c_0|^2 = |c_1|^2 = 1/\sqrt{2}$ and (f) shows a general, usually unknown superposition.

formed and the corresponding quantum state of the entire register must be considered. Clearly, this state can be, and generally is, in a superposition of all the pertaining states of the individual qubits. This generalizes the superposition concept that we commonly encounter in individual quantum systems to the entire system that seemingly consists of separate two-level systems. However, that point of view is no longer valid since even a manipulation of any one of the qubits in a row will change the quantum state of the entire system. Hence, the quantum register must usually be considered as entangled. Superposition and entanglement are the two features that generally distinguish a classical computer from a quantum computer and their control and manipulation will eventually enable one to speed up computational processes.

Analogous to a classical computer, a set of gate operations is required that allow one to formulate a calculation step by step. It has been shown in 1995 that two operations are sufficient to provide a universal set of quantum operations, i.e. that allow one to implement arbitrary computations.[7] Aside from the single qubit operation, which implements an arbitrary positioning and rotation of the arrow (see Fig. 1) given on the sphere, it is necessary to allow for conditional operations equivalent to the classical XOR operation in computer science. With such operations, the state of a target qubit can be changed depending on the state of a control qubit. The corresponding truth table is shown in Fig. 2 and looks exactly like the classical XOR operation, however, it needs to hold for all coherent superpositions. Thus,

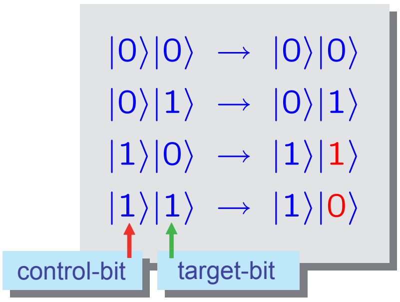

Fig. 2. Truth table of a CNOT-gate operation. The state of a target bit is flipped if and only if the control bit is in state "1". The notation indicates that this must hold for all superpositions.

the concept of a quantum computer can be visualized as shown in Fig. 3. Starting from an arbitrary input state

$$|x\rangle = \sum_{n\in\{0,1\}^m} c_n|n_1,\ldots,n_m\rangle, \quad \sum_n |c_n|^2 = 1\ , n_m \in \{0,1\}\ , \tag{2}$$

the computation works as a series of one and two-qubit operations according to the specific algorithm under consideration and the outcome is just another superposition $\mathcal{F}(|x\rangle)$ with an operation $\mathcal{F}$ that can be described by a unitary operator. To this point a quantum computation is completely reversible. The outcome of the calculation is then obtained by a measurement that projects the system on its eigenstates and yields classical information in terms of zeros and ones for the individual qubits.

The realization concepts of a specific quantum computer and its implementation vary widely depending on the quantum system considered, the quantum operations that are performed and the measurements that are taken to obtain classical information. On the other hand, there are a few building blocks and requirements that can be generally defined and described and that are common to all quantum computers. The requirements for a system to be considered for the implementation of a quantum computer are currently known as the so-called DiVincenzo criteria.[8] Irrespective of the specific system, a quantum computer clearly needs (1) storage sites for the quantum information, i.e. qubits that can be arranged to form a (scalable) quantum register, (2) the possibility to initialize the qubits to

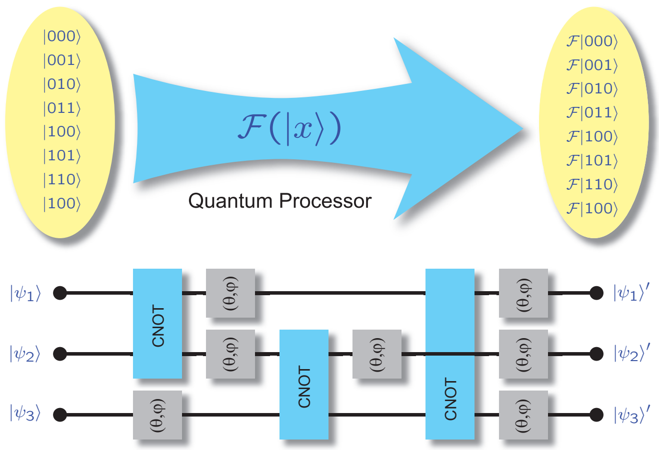

Fig. 3. Scheme of a circuit model quantum computer illustrated with 3 qubits. An arbitrary input superposition state $|x\rangle$ is processed with a series of one and two-qubit operations described by a unitary operation $\mathcal{F}(|x\rangle)$. (θ, φ) denote single qubit rotations, where (θ, φ) may vary from pulse to pulse depending on the algorithm.

arbitrary states, (3) long unperturbed computation (coherence) times, (4) a universal set of gate operations to allow for universal computations and (5) a highly efficient measurement of the qubit states to read out the result of the computation. In order to achieve large scale quantum computation, (6) the system under consideration should allow for a conversion between the stored, i.e. static and flying qubits that (7) can be faithfully transmitted between two quantum computer nodes.

During the last decade a large number of systems has been and still is investigated for its suitability to implement a quantum computer.[9] In particular, quantum optical systems of atoms and ions in traps, using the tools of laser spectroscopy, are among the most promising candidates for such a device.

4. Quantum computer with trapped ions

One of the first and seminal schemes to implement a scalable quantum computer was proposed by I. Cirac and P. Zoller in 1995.[10] They considered a string of laser cooled trapped ions in a Paul trap as quantum register and formulated how a CNOT-gate operation can be realized with laser pulses that individually address the ions. The crucial idea was that the harmonic motion of ions in the trap can be used as a quantum bus. That allows one to map the excited state of the controlling qubit to the motion and thus enables state manipulation of the target qubit conditioned on the motion and thus the controlling qubit. However, this requires that the ion string is optically cooled to the ground state of the harmonic oscillator which can be achieved in ion traps by sideband cooling.[11] Moreover, the state of laser cooled ions in traps can be detected with nearly 100% efficiency using the "shelved electron technique", where the absorption of a single photon results in a lack of a huge number of fluorescence photons on a monitoring transition.[11] As is well known from precision spectroscopy, trapped ions also offer extremely long coherence times[12] and therefore provide an ideal system for the implementation of a quantum computer. Fig. 4 shows schematically

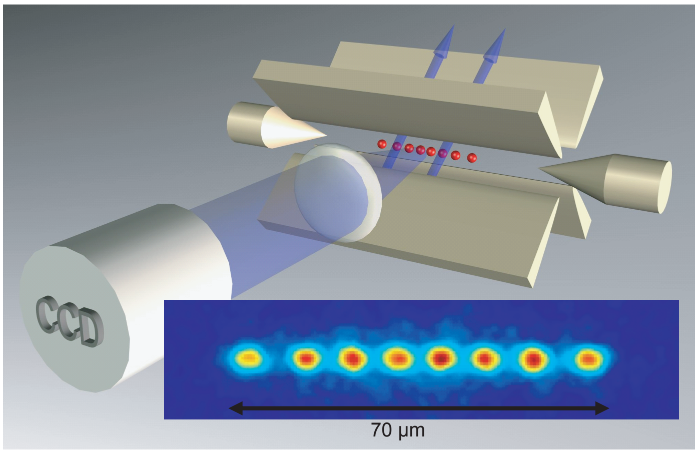

Fig. 4. Sketch of a linear ion trap holding a string of laser cooled ions that can be individually addressed for quantum state manipulation. With a CCD camera the fluorescence light is detected and allows for efficient state detection.

how a string of laser cooled ions is manipulated with focussed laser beams. State detection is achieved by observing resonance fluorescence with a CCD camera. With such setups, single qubit operations were performed, and CNOT-gate operations have been implemented with trapped ions[13–16] using the Cirac-Zoller idea as well as other proposals based on geometric phase changes.[17]

5. Simple quantum computations

With a small trapped ion quantum computer, both the Boulder[13] and the Innsbruck[14] groups have demonstrated simple quantum algorithms. As a basic building block, the CNOT gate operation (or an equivalent phase gate operation) was used to generate Bell states at the push of a button.[18,27] These subsequently could be used as a resource for a demonstration of the teleportation of an atomic state.[19,20] Non-classical entangled states of three particles, in particular the GHZ and W states were created[21,22] deterministically and analyzed using quantum state tomography.[27] A quantum Fourier transform was implemented[24] and error correction was demonstrated by the Boulder group.[25] Multi-partite entanglement was achieved and analyzed for a 6-ion GHZ state[23] and an 8-ion W state,[26] the latter demonstrating for the first time a quantum byte. This experiment for the first time also manifested the power of quantum computation: While the creation of an eight-ion entangled state takes just about 1 ms to achieve, its analysis via quantum state tomography required a lot more efforts. In order to obtain all density matrix elements (i.e. 256x256 entries) more than 6500 different qubit rotations had to be applied that took more than 10 hours of uninterrupted running time of the quantum computer. Moreover, the data analysis on a classical computer required a raw computing time of several days on a computer cluster. This clearly demonstrates that even with relatively few qubits highly complex states can be created.

6. Future developments

With the ion trap quantum computer quantum information processing clearly has become reality, albeit on a small scale yet. On the other hand, there exist already architectures to scale such a system up.[28] Of course, this still requires enormous efforts in physics and technology, especially in order to meet the requirements for error correction. While this is technically involved, there is however not a real roadblock in sight at this time. Therefore, current efforts are dedicated especially towards the development of yet smaller, so-called segmented ion traps that allow one to move the ions and thus the information around.[29] With such chip traps available, there is good hope for an even broader application of quantum information processing. In particular, the use of entanglement for precision spectroscopy[30,31] seems a very promising avenue for further enhanced measurements and sensor technology.

7. Conclusion

While the ion trap quantum computer seems farthest advanced at this time, it is quite foreseeable that other quantum optics and laser spectroscopy technologies, e.g. based on atoms in lattices, quantum dots, or superconducting qubits will become very strong alternatives soon. The steadily growing field of quantum information has enormously profitted from the fields of laser spectroscopy, laser cooling and precision measurements. On the other hand, quantum information processing provides us with new tools that allow us to further enhance our understanding of fundamental physics as well as to develop future devices.

References

1. G. Moore, Electronics **38**, Nr. 8, April 19, (1965); see also http://www.intel.com/technology/mooreslaw/.
2. R. W. Keyes, IBM J. R&D. V32, N1, Jan 1988, p.26
3. D. Deutsch, Proc. R. Soc. London A **400**, 97 (1985).
4. R. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).
5. P. W. Shor, Proceedings of the 35th IEEE Symposium on Foundations of Computer Science, pages 124–134. IEEE, 1994.
6. L. Grover, in Proceedings of the 28th Annual ACM Symposium on the Theory of Computation (ACM Press, New York, 1996), pp. 212219.
7. A. Barenco, C.H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. **52**, 3457 (1995).
8. D. DiVincenzo, Quant. Inf. Comp. **1** (Special), 1 (2001).
9. for the US roadmap see http://qist.lanl.gov/ and for the European roadmap see http://qist.ect.it/.
10. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).
11. D. Leibfried, R. Blatt, C. Monroe, and D. Wineland, Rev. Mod. Phys. **75**, 281 (2003) and references therein.
12. D. J. Wineland, C. Monroe, W. M. Itano, D. Leibfried, B. E. King, and D. M. Meekhof, J. Res. Natl. Inst. Stand. Technol. **103**, 259 (1998) and references therein.
13. D. Leibfried, B. DeMarco, V. Meyer, D. Lucas, M. Barrett, J. Britton, W. M. Itano, B. Jelenkovic, C. Langer, T. Rosenband, and D. J. Wineland, Nature **422**, 408-411 (2003).
14. F. Schmidt-Kaler, H. Häffner, M. Riebe, S. Gulde, G. P. T. Lancaster, T. Deuschle, C. Becher, C. F. Roos, J. Eschner and R. Blatt, Nature **422**, 412-415 (2003).
15. J. P. Home, M. J. McDonnell, D. M. Lucas, G. Imreh, B. C. Keitch, D. J. Szwer, N. R. Thomas, S. C. Webster, D. N. Stacey and A. M. Steane, New Journal of Physics **8**, 188 (2006).
16. P. C. Haljan, P. J. Lee, K-A. Brickman, M. Acton, L. Deslauriers, and C. Monroe, Phys. Rev. A**72**, 062316 (2005).
17. K. Mølmer and A. Sørensen, Phys. Rev. Lett. **82**, 1835 (1999); G. J. Milburn, S. Schneider, and D. F. V. James, Fortschr. Phys. **48**, 801 (2000).
18. Q. A. Turchette, C. S. Wood, B. E. King, C. J. Myatt, D. Leibfried, W. M. Itano, C. Monroe, and D. J. Wineland; Phys. Rev. Lett. **81**, 3631 (1998).

19. M. Riebe, H. Häffner, C. F. Roos, W. Hänsel, J. Benhelm, G. P. T. Lancaster, T. W. Körber, C. Becher, F. Schmidt-Kaler, D. F. V. James, R. Blatt, Nature **429**, 734 (2004).
20. M. D. Barrett, J. Chiaverini, T. Schaetz, J. Britton, W. M. Itano, J. D. Jost, E. Knill, C. Langer, D. Leibfried, R. Ozeri and D. J. Wineland, Nature **429**, 737 (2004).
21. C. F. Roos, M. Riebe, H. Häffner, W. Hänsel, J. Benhelm, G. P. T. Lancaster, C. Becher, F. Schmidt-Kaler, R. Blatt, Science **304**, 1478 (2004).
22. D. Leibfried, M. D. Barrett, T. Schaetz, J. Britton, J. Chiaverini, W. M. Itano, J. D. Jost, C. Langer, and D. J. Wineland, Science **304**, 1476 (2004).
23. D. Leibfried, E. Knill, S. Seidelin, J. Britton, R. B. Blakestad, J. Chiaverini, D. B. Hume, W. M. Itano, J. D. Jost, C. Langer, R. Ozeri, R. Reichle and D. J. Wineland, Nature **438**, 639-642 (2005).
24. J. Chiaverini, J. Britton, D. Leibfried, E. Knill, M. D. Barrett, R. B. Blakestad, W. M. Itano, J. D. Jost, C. Langer, R. Ozeri, T. Schaetz,ddagger D. J. Wineland, Science **308**, 997-1000 (2005).
25. J. Chiaverini, D. Leibfried, T. Schaetz, M. D. Barrett, R. B. Blakestad, J. Britton, W. M. Itano, J. D. Jost, E. Knill, C. Langer, R. Ozeri, D. J. Wineland, Nature **432**, 602-605 (2004).
26. H. Häffner, W. Hänsel, C. F. Roos, J. Benhelm, D. Chek-al-kar, M. Chwalla, T. Körber, U. D. Rapol, M. Riebe, P. O. Schmidt, C. Becher, O. Gühne, W. Dür and R. Blatt, Nature **438**, 643-646 (2005).
27. C. F. Roos, G. P. T. Lancaster, M. Riebe, H. Häffner, W. Hänsel, S. Gulde, C. Becher, J. Eschner, F. Schmidt-Kaler, R. Blatt, Phys. Rev. Lett. **92**, 220402 (2004).
28. T. S. Metodi, D. D. Thaker, A. W. Cross, F. T. Chong, I. L. Chuang, arXiv:quant-ph/0509051v1.
29. D. Kielpinski, C. Monroe, D. J. Wineland, Nature **417**, 709-711 (2002).
30. P. O. Schmidt, T. Rosenband, C. Langer, W. M. Itano, J. C. Bergquist, and D. J. Wineland, Science **309**, 749-752 (2005).
31. C. F. Roos, M. Chwalla, K. Kim, M. Riebe, R. Blatt, Nature **443**, 316-319 (2006).