

QUANTUM INFORMATION

Reality check

Liesbeth Venema

It will be a long experimental haul before the great potential of quantum effects can routinely be exploited for technological ends. A sense of practical purpose among researchers will encourage progress.

When the citizens of Geneva cast their votes in the Swiss federal elections on 21 October, they could be confident that their ballots were safe — thanks to the rules of quantum mechanics. The poll results were sent down an optical fibre from the counting station to a government data centre, and their integrity was safeguarded by a quantum encryption key transmitted through the same fibre. Such a key promises to be 100% secure. It is composed of a stream of single photons that each take a random, unpredictable polarization state, and any attempts at tampering or eavesdropping will be noticed by the sender and receiver.

Quantum cryptography was high on the agenda at a meeting* last month on quantum information technology. Whether or not the exercise in Geneva was genuinely motivated by security concerns, it demonstrates, as a first public deployment of quantum cryptography, that the technique is ready to enter the commercial market for data encryption (G. Ribordy, id Quantique, Geneva; J. Dubois, Senetas, Melbourne). But a recurring theme of the meeting was the pressing requirement to identify other areas of practical application for quantum-information systems.

Another major prospect is quantum computing. Quantum computers will not simply be faster versions of the computers we have today. Rather, they will carry out tasks that are hard to tackle with any classical approach: for example, factoring large numbers and searching databases. Algorithms for such tasks have been available for more than a decade, and it is realizing the hardware that remains the main barrier to progress.

The building-block of a quantum computer is the qubit, a versatile version of the conventional bit. Like its classical counterpart, a qubit has two well-defined levels, '0' and '1'. But it also has the curious property that it can be in both states at the same time, occupying them with a certain probability. This phenomenon, known as 'superposition', in principle offers a powerful way to perform calculations because several logic operations can be carried out

simultaneously. Another useful property of qubits is that they can be entangled — that is, their states can be prepared so that they are correlated to each other, even though each is unknown. For example, if one qubit happens to be in level 0 the other one will occupy level 1, and vice versa. The exact outcome becomes fixed as soon as either of the two is measured.

A wide range of qubit designs — based on atoms, ions, electrons, photons and even superconducting currents — was highlighted at the meeting. In most cases, at least two qubits can now be connected so that some sort of logic operation can be carried out. In one of the most advanced approaches, in which qubits take the form of ions trapped in an electromagnetic field, up to eight qubits have been entangled with each other. A new experimental development is the construction of a so-called Toffoli logic gate with ion qubits (R. Blatt, Univ. Innsbruck). Toffoli gates are a familiar concept in classical computation, but are the subject of renewed interest because they may offer a solution to error correction, a crucial consideration for quantum computers. However, they require three inputs and are therefore more difficult to realize than the two-qubit logic gates demonstrated so far.

The main problem with qubits is that their quantum states are fragile, and quickly leak away into the environment. This raises the scaling issue. Coupling just a few qubits together seems feasible. But as an increasing number of them are connected, more quantum leaks occur, so that information is quickly lost. Part of the solution may lie in using photons, relatively robust quantum entities, to channel quantum information between remote qubits, and experimental work is under way to construct such optical quantum connections. Instead of building a computer of say, 5,000 qubits, a more realistic goal may be to optically connect 1,000 quantum registers of just five qubits — one for storage, one for communication and three auxiliary qubits to ensure fault tolerance (A. Sorensen, Niels Bohr Inst., Copenhagen)¹.

Small-scale quantum computers, designed to carry out a specific task, could be just a few years away. But a take-home message from the meeting was that more immediate applications of quantum technologies are urgently required to keep industrial partners interested (T. Spiller, Hewlett-Packard, Bristol). The 'killer application' for quantum information is not yet known, and more practical ideas need to be generated to kick-start a new market². It is sobering to realize that the inventors of the transistor did not foresee the huge integrated-circuit industry that would develop; their first

"The 'killer application' for quantum information is not yet known, and more practical ideas need to be generated to kick-start a new market."

idea for a useful application of transistors was in hearing aids. What we need to bootstrap quantum-information technology, says Spiller, are quantum hearing aids.

When it comes to near-future technological applications, quantum communication, and quantum cryptography in particular, seems to be the best bet. The record distance over which a quantum key has been transmitted, both through an optical fibre and through free space, is about 150 km. But if quantum-communication technology is to be widely developed, it will be necessary to improve efficiency. At the meeting there was much talk of 'quantum repeaters' — pieces of hardware that can temporarily store and release photons without losing their quantum states, and that are seen as essential for the effective distribution of quantum information over large networks and distances. The experimental challenge to construct quantum repeaters is probably on a par with the challenge to generate practical qubits. So far, quantum memories, the basic element of a quantum repeater, have been made from ensembles of cold gaseous atoms. But a solid-state form will eventually be required: atomic ensembles of rare-earth ions, inserted in a nonlinear optical waveguide, are among the first candidates to be investigated (M. Staudt, Univ. Geneva)³.

The quantum future looks bright, although it will take a sustained experimental push before basic effects such as entanglement, inherent randomness and superposition can be exploited

*QIPC 2007: International Conference on Quantum Information Processing and Communication, 15–19 October 2007, Barcelona, Spain.

in real devices (practical or otherwise). But although quantum mechanics has been one of the most successful theories of the past century, nobody can confidently claim to understand why it works so well; for instance, how two entangled particles seem to communicate with each other at a distance, without any interaction, is beyond anybody's comprehension. There is a nagging feeling that we are missing something. A quantum-information industry may indeed

be just around the corner, but its underlying principles remain largely mysterious. ■

Liesbeth Venema is a senior editor at *Nature*.
e-mail: l.venema@nature.com

1. Jiang, L., Taylor, J. M., Sorensen, A. S. & Lukin, M. D. preprint at <http://arxiv.org/abs/quant-ph/0703029> (2007).
2. Spiller, T. P. & Munro, W. J. *J. Phys. Condens. Matter* **18**, V1-V10 (2006).
3. Staudt, M. U. *et al. Phys. Rev. Lett.* **99**, 173602 (2007).

COMPUTATIONAL BIOLOGY

Protein predictions

Eleanor J. Dodson

Predicting the three-dimensional structure of a protein from its amino-acid sequence is a dauntingly complex task. But with colossal computer power and knowledge of other structures, it can be done.

Fifty years have passed since the Nobel-prizewinning discovery that the amino-acid sequence of a protein determines its three-dimensional structure¹ — yet computational biologists are still unable to predict the shape of a protein from its sequence. Given that there are many more protein sequences available than structures, and that protein shape is crucial for understanding cellular and physiological processes, a method for predicting such structures is vital. The paper by Qian *et al.*² (page 259 of this issue), in which the structure of a protein containing 112 amino acids is accurately predicted, thus represents a real breakthrough*. The authors' model was sufficiently accurate to act as the starting point in the X-ray structure determination of the protein.

Most structural information on proteins is derived from X-ray and nuclear magnetic resonance (NMR) experiments. These have revealed the general characteristics of proteins — for example, sequence motifs that form secondary structural elements such as helices and sheets. Such elements are organized to generate the overall protein architecture, mainly as a result of internal interactions between hydrophobic amino-acid side chains buried within the structure.

The shape of a protein corresponds to the lowest-energy conformation of that molecule and reflects the combined properties of the constituent amino acids. Low-energy conformations arise when the 'backbone' peptide chain is tightly packed into secondary structural features. Such packing exploits both the hydrogen-bonding of amino-acid side chains to each other and the energetically favourable, compact patterns that arise from hydrophobic interactions. Several crucial

side-chain interactions are almost always found in certain structural elements of proteins, but in general there is no simple correlation between amino-acid sequence and protein structure; quite different sequences can adopt very similar folds.

Once a protein structure is known, it is fairly easy to see the atomic interactions that underpin it. But it is much harder to take an amino-acid sequence and work out the optimal interactions that determine how it will fold. First, it is necessary to quantify the energy contributions from various types of

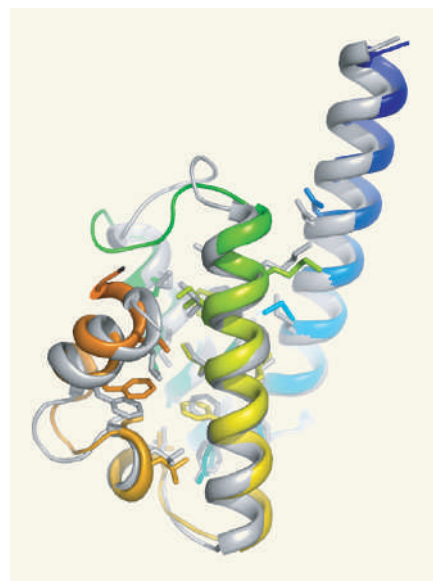


Figure 1 | Model test. Qian *et al.*² have developed a computational method for predicting the three-dimensional structure of a protein from its amino-acid sequence. Here, their predicted structure (grey) of a protein is overlaid with the experimentally determined crystal structure (shown in colour) of that protein. The agreement between the two is excellent, with the amino-acid side chains overlapping particularly well.

interaction. The effects of molecular conformations on these contributions must then be assessed. But even a relatively small protein can have a bewilderingly large number of possible conformations. Although some progress has been made towards devising a structural prediction method, crystallographers have so far had no reason to worry about their job security.

The field was greatly stimulated by a network set up in 1994 to provide a critical assessment of structure prediction (CASP)³. The main goal of the CASP network is "to obtain an in-depth and objective assessment of our current abilities and inabilities in the area of protein structure prediction"⁴. Every two years the organizers provide the amino-acid sequences of a set of proteins for which undisclosed crystal structures exist. Modellers are challenged to predict structures for the proteins, and these are then assessed against the crystallographic results. The assessors use various scoring systems, but the most rigorous test is the one used by Qian *et al.*² to test their own models — can the prediction be used in 'molecular replacement' searches⁵ that allow the raw data from X-ray diffraction studies to be related to the structure of the compound being investigated? Normally, a previously determined structure of a protein with a similar amino-acid sequence is used for this purpose.

Qian and colleagues' models² passed the molecular-replacement test with flying colours (Fig. 1): one of the authors' *ab initio* predictions was used successfully as a molecular-replacement model. Furthermore, the authors used their method to refine ten NMR models of protein structures, yielding results that were in better agreement with X-ray data than the original models. And finally, they were able to improve the molecular-replacement scores of several models that started from protein structures distantly related to that of the target protein. This gives the lie to the old crystallographers' adage that computational modelling is a time-consuming way to make a poor model worse.

The authors used a program called Rosetta to make their structural predictions. The program begins by mapping fragments of the sequence under review against existing information from previously determined structures, to identify likely structural motifs. It then constructs many rough, low-resolution models from these fragments and tests them against energy criteria (which are dominated by hydrophobic interactions). In this way, a large set of possible low-energy conformations is identified, one of which is likely to be that adopted by the protein.

At the next stage, the energy profile of every atom in the protein is incorporated into the low-energy models. Rosetta explores a huge range of randomly generated side-chain and backbone conformations, again calculating their effects on molecular energy. The resulting energy 'landscape' can vary dramatically — for example, small shifts of a single atom can make or break a hydrogen bond.

*This article and the paper concerned² were published online on 14 October 2007.