NATURE|Vol 436|4 August 2005

50 & 100 YEARS AGO

50 YEARS AGO

Recent investigations have shown that some of the free amino-acids in amphibian embryos change in concentration during early development. These changes are of interest because they may be related to the synthesis of new, specific proteins...it is possible to carry out analyses of the free amino acids not only in whole embryos but also in different regions representing different tissue primordia. Any regional differences in free amino-acid content which might be related to the early synthesis of tissue-specific proteins can in this way be detected. The results already quoted indicate that at least dorsoventral regional differences do exist.

From *Nature* 6 August 1955.

100 YEARS AGO

It is sometimes said that natural selection has ceased as regards civilised man; but very clearly this is an error. All civilised and most savage races are very stringently selected by various forms of zymotic disease. Thus in England practically everyone is brought into contact with the organisms which give rise to tuberculosis, measles and whooping-cough. Abroad, malaria, dysentery, and many other complaints play a similar *rôle*...The result of all this elimination by diseases demonstrates natural selection very beautifully. Every race is resistant to every disease strictly in proportion to its past experience of it...These facts appear to establish conclusively two truths, first that evolution is due solely to natural selection, and second that variations, except, perhaps, in rare instance, are not due to the direct action of the environment on the germ-plasm, but are "spontaneous." The Lamarckian doctrine is quite out of court. If ever acquirements are transmitted, it should be in the case of the profound and lasting changes affecting the whole body which result from disease; but in no instance is the effect produced by any disease on the race similar to that produced by it on the individual.

From *Nature* 3 August 1905.

The gap between what was provided at first (four letters), and what allowed us to decipher the sentence (no more than ten letters) illustrates the notion of 'conditional uncertainty' — the amount of extra information required to decipher a message.

One of Shannon's seminal results[1] was to find a simple formula for the uncertainty of a data source X. This function, usually written $H(X)$, is known as the Shannon entropy of X. Conditional uncertainty can be represented in similarly simple terms. If Y is used to represent the information already given to the receiver — the analogue of the indecipherable four letters in our example — the amount of extra information that must be provided is $H(X,Y) - H(Y)$, a quantity known as the conditional entropy of X given Y (ref. 3).

This second formula is easy to interpret: the extra information required is equal to the uncertainty in the total message, consisting of both X and Y, minus the uncertainty owing to Y alone, which should be subtracted, as Y is already known.

Among its many intuitive features, the conditional-entropy function is always greater than or equal to zero. That's because there is potentially more to be ignorant of in two messages X and Y together than in Y alone, so the inequality $H(X,Y) \geq H(Y)$ holds. For example, X and Y could represent future issues of the *Financial Times* and *The Wall Street Journal*, respectively: readers who take the time to follow both newspapers will be intimately familiar with the practical meaning of the inequality! In the context of conditional uncertainty, the interpretation is again highly intuitive: the amount of extra information required to decipher a message cannot be less than zero bits or, equivalently, it is impossible to be more than certain about the outcome of an event.

Intuitive indeed, but alas no longer true in quantum information theory. Horodecki, Oppenheim and Winter analyse[2] a quantum-mechanical version of the message-completion problem and find that the amount of extra information required can sometimes be less than zero qubits (a qubit is simply the quantum version of a bit). In their version of the problem, there are three participants: call them the sender, the receiver and the referee. The referee prepares a quantity of quantum information consisting of many particles, some of which he distributes to the sender and the receiver, and the rest he keeps for himself. The sender's job is to find an encoding that allows her to transfer her share of the information to the receiver using as few qubits as possible. To further isolate the quantum-mechanical features of the problem, the sender is also allowed to send old-fashioned messages consisting of bits at zero cost.

The authors show[2] that the number of qubits that the sender needs to transmit is precisely $S(A,B) - S(B)$, where A now refers to the sender's particles, B to the receiver's particles and S is the von Neumann entropy, a direct quantum-mechanical generalization of Shannon's entropy. This formula is identical in form to the solution of the non-quantum version. With quantum particles, however, it is possible for A and B to be correlated in ways that are impossible in the classical situation[4]. In such cases, the systems A and B are said to be entangled (for a popular account of this phenomenon, see ref. 5). One consequence of entanglement is that conditional uncertainty, $S(A,B) - S(B)$, can sometimes be less than zero. In other words, the receiver can be more than certain!

In practice, if the receiver is more than certain, the sender doesn't need to transmit any qubits at all for the receiver to be able to decipher the message. So the receiver can put some certainty in the bank for a rainy day, in the form of extra entanglement with the sender that could be used to reduce the receiver's uncertainty about future messages. Entanglement is such a strong form of correlation that it can actually be used to send qubits from the sender to the receiver using a procedure known as quantum teleportation[6]. On the accounting ledger, therefore, having stored entanglement is almost as good as being able to communicate.

This neat and satisfyingly bizarre resolution disposes of a long-standing puzzle in quantum information theory: put simply, how to quantify who knows what. In more technical language, the puzzle was how to quantify conditional uncertainty. The formula $S(A,B) - S(B)$ had been proposed[7], but was widely rejected because of its pathological tendency to become negative. Until now, no one had succeeded in finding a setting in which the formula's full range of positive and negative values would have a meaningful interpretation. (It was a quantum-information theorist's version of the famous conundrum from *The Hitchhiker's Guide to the Galaxy*: if 42 is the answer to Life, the Universe and Everything, what is the question?)

In addition to finally placing the quantification of uncertainty in quantum mechanics on a solid footing, the new result[2] opens the door to solving many previously intractable problems in quantum information theory. The authors provide a sampling of these applications in their paper, including an easy solution to a quantum version of the problem of many cellphones trying to communicate simultaneously to a single base station[8]. This astonishing solution shows that one sender's quantum information can, despite its fragility, be used to help decode the other senders' transmissions at higher rates than would otherwise be possible. Once again, quantum information has proved to be more versatile and more surprising than anyone expected. ■

Patrick Hayden is in the School of Computer Science, McGill University, 3480 University Street, Montreal, Quebec H3A 2A7, Canada.
e-mail: patrick@cs.mcgill.ca