REVIEWS

Get set for the quantum revolution

To cite this article: Anton Zeilinger 1997 *Phys. World* **10** (9) 54

somewhat surprising that the programme relies so heavily on computer graphics that seem to have been generated specifically for the series rather than based on real images. The most exciting aspect of cosmology in recent years has been the flood of new images and data.

Readers of *Physics World* will be familiar with most of the ground covered, and will probably find the series rather slow moving – especially the early episodes. But the series is not aimed at physicists and astronomers, and given the success of *A Brief History of Time* – and Hawking's reputation as a gambler – I would not bet against it being a success in the ratings.

Peter Rodgers is editor of *Physics World*

Anton Zeilinger

Get set for the quantum revolution

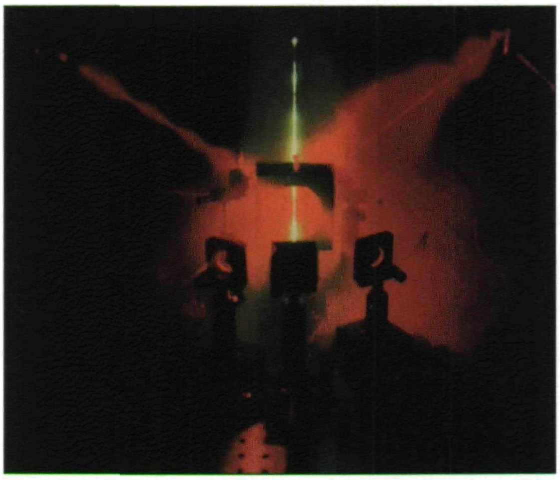
Schrödinger's Machines: the Quantum Technology Reshaping Everyday Life 1997 Gerard Milburn W H Freeman and Company 188pp $21.95hb

WE ARE currently in the midst of a boom in experimental and theoretical work related to the foundations of quantum physics. This delightful book by Gerard Milburn, which draws many different strands of these activities together, shows how this work is leading to the emergence of completely new technology – related to quantum computing, communication and cryptography.

This new technology has a rather strange history. Quantum physics was invented in the 1920s to explain the spectra emitted by objects as diverse as atoms and black bodies. However, from the beginning people realized that some of the consequences of the theory were completely counterintuitive. This was initially demonstrated in many beautiful "thought experiments", which were used by giants such as Bohr, Einstein, Heisenberg and Schrödinger to illustrate particular theoretical points. But technological progress over the last twenty years has since allowed us to actually do many of these thought experiments in the laboratory. Indeed, it is now everyday practice to experiment with individual photons, electrons and atoms.

However, our ability to physically do these thought experiments has not only let us demonstrate many of the counterintuitive features of quantum physics, it has also opened the door to a wealth of new phenomena that, as Milburn points out, have triggered the new technology he describes in this book. Basic human curiosity has led to technological progress that was not envisaged by those who were just trying to solve some of the most burning issues, like the nature of reality, our role in the world and what it means for an object to be here, not there.

In "Quantum Roulette" – the first of the book's six chapters – Milburn beautifully illustrates how randomness plays a completely different role in quantum physics than it does in classical physics. In doing so, he also introduces us to the notion of a quantum bit or "qubit", probably one of the most important concepts in the new field of quantum information technology. In the next chapter, "Atomic Calligraphy", we are introduced to the idea of tunnelling and its application in the scanning tunnelling microscope, which was developed by Gerd Binnig and Heinrich Rohrer at IBM's Zurich laboratory in the early 1980s. Milburn's description of how the researchers approached the problem and how they overcame enormous experimental difficulties is a gem. The term calligraphy refers to the idea of atom-craft, in which new technology allows individual atoms to be placed at will on a surface.



Easy does it – a two-photon "quantum eraser" can alter the state of individual photons using conventional optics

The author continues his discussion of how to manipulate atoms in the third chapter, where we learn how atoms can be trapped using laser beams. This technique cools atoms to temperatures far lower than would otherwise be possible, and I believe that the application of these ideas of atom optics to write nano-scale devices will lead to a technological revolution.

Chapter 4, entitled "Quantum Nanocircuits", introduces us to more conventional electronic circuits based on semiconductor devices, but constrained to such small dimensions that quantum effects are important. Before he tackles quantum phenomena, the author carefully presents the so-called "single-electron turnstile devices", in which the electric current can be manipulated electron by electron. Milburn is at pains to point out that these phenomena are not yet part of the quantum world; rather they are based on the fact that charge only comes in discrete pieces, namely multiples of the charge of the electron. The second half of the chapter presents us with the idea of a quantum interference transistor, and in passing we also learn about two-dimensional electron gases in semiconductors and about the Aharonov–Bohm effect, which can actually control the current in a quantum interference transistor.

In chapter 5, "Quantum Cryptography", we first learn about classical methods of encrypting messages and the limits involved. The most interesting and most widely used method is the RSA algorithm, invented by Ronald Rivest, Adi Shamir and Leonard Adleman at the Massachusetts Institute of Technology in the US. The algorithm is based on the fact that it is very difficult to factorize a large number into its prime numbers – the time needed to factorize a number increases so rapidly with the size of the number that it is easy to invent a number big enough that it cannot be factorized within a reasonable time.

One problem with this idea is that it has not yet been proved – someone could, in principle, devise a clever algorithm that would allow a conventional computer to factorize large numbers much faster than we can currently achieve. The second – and probably more important – problem is that a quantum computer, if it existed, could do the job very much faster than all of the machines we have today. For cryptologists, the way out of this problem is to rely on the Heisenberg uncertainty principle, which basically makes it impossible for an eavesdropper to "listen" to the information without disturbing the quantum state of the qubits sent from Alice to Bob, as the sender and recipient are conventionally named.

But physicists have proved that quantum cryptography can work – even with existing telecommunication fibres – and I find it hard to understand why Milburn is not more optimistic about its practical implications. I also cannot agree with his statement that "it requires an entire laboratory of state-of-the-art laser equipment to make it work". In fact, everything we need for quantum cryptography can easily be fitted onto a PC card, and a number of laboratories in Switzerland, the US, Austria and the UK are trying to make this work.

One experimental goal that probably lies further into the future is the quantum computer, which is covered in chapter 6. Using very simple language, the author explains ideas such as algorithmic complexity and how to define the randomness of a number – an idea first introduced by Gregory Chaitin. Defining randomness is particularly hard if you realize that, as far as we know today, any sequence of numbers we care to write down is contained somewhere in the decimal expansion of π. Consider, for example, the sequence 445923078. It may look quite random, but it is just the value of π between the 49th and the 57th decimal place. Milburn then talks about "reversible computation" and "elementary gates", before he introduces us to the marvellous idea of the square-root-of-NOT-gate, first devised by David Deutsch and Richard Jozsa. The chapter concludes with a brief discussion of what a quantum computer could actually achieve. Milburn calls for all these technologies to be brought together in the hope that someone, someday, may create a Department of Quantum Engineering. I agree that this is an idea whose time has come.

All in all, this is a formidable book, in which the author presents an admirable tour de force through a completely new field. The huge technological progress he describes may best be understood by comparing this book with the marvellous *Mr Tompkins in Quantum Land* by the inventor of quantum tunnelling, George Gamow. First published in 1940, Gamow had to use some rather artificial examples to demonstrate the strangeness of quantum mechanics. Today, however, we have many real experiments and emerging new technology.

If there are any shortcomings to this book, then the most serious – apart from the fact that newcomers to the field might find it difficult – is that it probably is not radical enough. As I mentioned above, I cannot agree with Milburn about the difficulty in getting quantum cryptography to work, and I also do not understand why he does not mention quantum entanglement, which is probably one of the most radical things about quantum mechanics. In fact, as Jozsa recently showed, a quantum computer can only reach its immense speed by drawing heavily on quantum entanglement: without entanglement, the quantum computer would not achieve anything remarkably new. To be fair to the author, the problem is that the field is developing so fast that a book written today, finished tomorrow and sold the day after will already be out of date.

Writing in the introduction, Paul Davies convincingly suggests that while our time may be characterized as the "information age", the 21st century will be the true "quantum age". And Milburn, quoting John Wheeler, proposes that quantum mechanics is just a peculiar form of information science. If this idea is correct, and I certainly think it is, our century will justly be regarded as the prehistoric age of information science. The next millennium is when the real work will be done, and anyone who wants to be armed for the coming technological revolution must, I believe, read Gerard Milburn's beautiful book.

Anton Zeilinger is director of the Institut für Experimentalphysik, Universität Innsbruck, Austria

Roger Blin-Stoyle

Great physicists make great stories

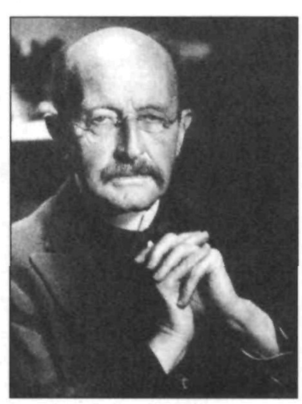
Heisenberg *Probably* Slept Here: The Lives, Times and Ideas of the Great Physicists of the 20th Century Richard Brennan 1997 John Wiley and Sons 274pp £17.99hb

PHYSICS has been around for a long time – the author of this book goes back to the Greek scholar Thales in the 6th century BC – and in that time our understanding of the physical world has lurched forward in fits and starts. But in the 20th century our knowledge has advanced at such a furious pace that people now talk with increasing regularity and confidence about the possibility of a "final theory".

Our understanding has grown in all three of the areas into which physics can crudely be divided – the very small, the very large and all that lies between. At the very small level are the elementary particles and their interactions. At the very large are the stars, the galaxies and the universe itself, while in between lie atoms, molecules and everyday matter. Of course, the very small and the very large are intimately connected. After all, the universe began with the big bang, when elementary-particle interactions critically affected what followed at larger scales.

To be able to understand the two extremes, we need fundamental theories that can unify the gravitational, the weak, the electromagnetic and the strong interactions – together with quantum mechanics and relativity. The intermediate region of physics, meanwhile, needs theories to deal with many-body complexity, essentially within the framework of quantum electrodynamics.

Although thousands of physicists have helped to push forward our knowledge in these areas this century, the input of some has, inevitably, been outstanding. This book is about seven such scientists: Einstein, Planck, Rutherford, Bohr, Heisenberg, Feynman and Gell-Mann. The author calls them "great" physicists, and who would argue with that? All were Nobel prize-winners, although in Rutherford's case the award was, curiously, for chemistry.


Ambivalent? – Max Planck

Brennan introduces us to their personalities – warts and all – and gives us a taste of their contributions to physics. But before embarking on this task, he takes us briefly through the early history of physics. He describes some of the work of the "giants", on whose shoulders Newton stood "to see further than other men". As well as Thales, these giants included Pythagoras, Euclid, Aristarchus, Archimedes, Eratosthenes, Copernicus, Kepler and Galileo.

Newton (a "pre-eminent scientific genius" in the eyes of the author) is given a whole chapter to himself, and here we learn about his famous contributions to our understanding of gravity, colour and the dynamics of motion – as well as light, telescopes and calculus. We are also told about Newton's "neurotic personality", his friendships with the philosopher John Locke and the writer Samuel Pepys, and his "angry, unreasonable attitude towards rivals", particularly his quarrels with Robert Hooke and John Flamsteed.

The author then moves on to the seven 20th-century physicists, providing some fascinating anecdotal insights into their characters and interests, as well as their concerns outside physics. We are told, for example, about Einstein's attitudes towards war and the atomic bomb, Rutherford's boisterous yet friendly personality, and Planck's potential as a professional musician and his difficult interaction with the Nazi regime. The author examines Bohr's relationships with Rutherford and Einstein – and his diffi-