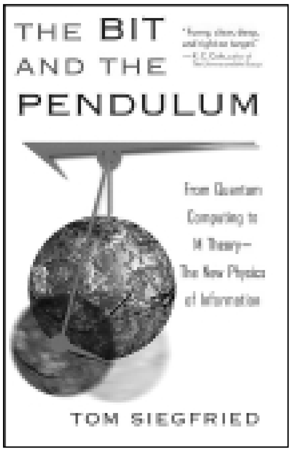
The Bit and the Pendulum

Reviewed by Solomon W. Golomb

The Bit and the Pendulum
Tom Siegfried
John Wiley & Sons, Inc., 2000
ISBN 0-471-39974-4
vi + 281 pp., $15.95 (paperback)

As a science journalist rather than a scientist, the author of this book aims to make contemporary research results and theories in a broad range of the physical sciences accessible to the general intelligent reader rather than to espouse idiosyncratic views of his own. As a unifying theme, he has chosen the digital computer and the information bit as conceptual models for various areas of science. He quotes John R. Pierce as saying, "Many of the most general and powerful discoveries of science have arisen, not through the study of phenomena as they occur in nature, but, rather, through the study of phenomena in man-made devices, in products of technology. This is because the phenomena in man's machines are simplified and ordered in comparison with those occurring naturally, and it is these simplified phenomena that man understands most easily."

Siegfried then observes that starting in the early fourteenth century, mechanical clocks made their appearance in Europe and were steadily improved over the years. Thus, when Newton's *Principia* appeared in 1687, the metaphor that was quickly adopted was that the universe operated like clockwork. (Models of the solar system were built using clockwork, obscuring the fact that planetary motion in the real universe is free of cogs and wheels and gear teeth.) In the mid-nineteenth century, with the steam engine ushering in the Industrial Revolution, the most important science became thermodynamics, and everything from biology to cosmology was redescribed in terms of the Law of Conservation of Energy. For the past fifty years the information age, with digital communications and computers, has transformed our world, and it is no surprise that many areas of science are now described in terms of information processing and computer models.



Imposing a unifying theme on the disorderly state of scientific research across many disciplines is not without its hazards. Siegfried offers the viewpoint that every chemical reaction can be regarded as a computational process, and the functioning of every bodily organ involves information processing on a monumental scale. While this description is certainly not false, it focuses away from those areas usefully modelled by the types of computers and information systems with which we are more familiar. Fortunately, Siegfried does not

Solomon W. Golomb is University Professor and Andrew and Erna Viterbi Professor of Communications at the University of Southern California. His e-mail address is `milly@usc.edu`.

unduly belabor these analogies. In the other direction, having introduced the possibility of quantum computing, he utilizes the opportunity to inform the reader of the bizarre nature of quantum reality in considerable detail, even where it has little to do with computation per se. For me, this was probably the most interesting part of the book. Does "quantum reality" require an unlimited number of parallel universes, continuing to multiply each time a quantum ambiguity arises, with each possible resolution giving rise to a different universe? (This is the popularized version proposed in the 1957 doctoral dissertation of Hugh Everett III.) This view has been in decline since the 1985 publication of a paper by Erich Joos and H. Dieter Zeh on "quantum decoherence", asserting that as an object (even a subatomic particle) interacts with its environment the quantum possibilities rapidly narrow down to *one*, and the larger the object, the faster the elimination of possible states. The "consistent histories" notion of quantum reality, introduced by Robert Griffiths in 1984, has been refined and extended by Murray Gell-Mann and Jim Hartle to allow some quantum ambiguities to persist for longer periods of time, provided that interactions with the external world are avoided. In fact, it is this possibility of maintaining quantum ambiguity for seconds or minutes (or even longer) that is necessary for quantum computing to attack any but the most trivial problems. So there is a tie-in back to computing after all, though Siegfried neglects to emphasize this in his "Quantum Reality" chapter. Also interesting in this chapter is the discussion of the "Copenhagen interpretation" of quantum mechanics, introduced by Niels Bohr in the 1920s, which seemed to require an intelligent observer in order to resolve possible quantum outcomes. In the view of Gell-Mann–Hartle and most others, all that is required is interaction with photons (or other "particles") to eliminate the quantum ambiguities.

Even more mysterious than the notion that "reality" could not exist without intelligent observers (a much older version was whether the tree falling in the forest made a sound if there was no one to hear it) was the "anthropic principle", which in its strong form asserts that the universe itself could not exist without (intelligent) life and even in its weak form marvels that the universe had to have precisely the physics that it does have in order for even galaxies, let alone life-supporting planets, to come into existence. To his credit, Siegfried observes that few scientists today would endorse the strong form, and influential people like Heinz Pagels and Martin Gardner regard the anthropic principle as "a sham, an intellectual illusion that has nothing to do with empirical science" (in Pagels' words). Yet Siegfried fails to distinguish Robert Dicke's perfectly reasonable observation that the reason certain physical phenomena are as they are arises from the fact that were they otherwise, we (or any life similar to ours) would not be around to observe them. I think it is unfair to credit, or blame, Dicke for originating either the weak or the strong form of the anthropic principle as Siegfried states them, with their teleological, if not theological, overtones, when Dicke's anthropic principle merely asserts that certain conditions will necessarily be present in the type of universe that gave rise to *us*.

A fascinating tie-in between quantum mechanics and "information", which Siegfried discusses at length, is: What happens to all the information in an object that gets swallowed up by a black hole? Here is an area where general relativity and quantum mechanics appear to be in conflict. General relativity says that no property except its mass "survives" (in the sense of being measurable) when the object enters the black hole, but quantum mechanics is understood to say that information about the past is never supposed to disappear. John Archibald Wheeler, who coined the term "black hole" in 1967 (though the use of this term in connection with Calcutta began much earlier), challenged Jacob Bekenstein in 1970 to resolve this paradox. Shortly afterward, Bekenstein responded that black holes have *entropy* as well as mass, and (as Claude Shannon discovered in 1948) entropy is in some sense the same as information. The surface area of a black hole is proportional to its entropy, and Wheeler views the entire surface as being filled with information bits. Of course, the reconciliation of general relativity with quantum mechanics is one of the greatest unsolved problems of contemporary physics, and having the "bits" on the surface of the black hole still leaves them inaccessible to the world outside the black hole.

Shannon's "bit" of information is the amount of information gained upon learning the answer to a yes-or-no question when both answers are equally likely a priori. Is a bit therefore a mathematical abstraction, like the number 43, or a physical object, like an atom or a chair? (Immanuel Kant distinguished the *physical* reality of the chair from the *transcendental* reality of 43, an improvement on Plato's view that just as "43" is an idealization from any actual set of 43 objects, any physical chair is merely the imperfect representation of the "ideal" chair residing in the same never-never land as prime numbers and perfect geometric circles.) Since we store bits in computer memories and transmit bits over communication channels, they seem to have some physical reality, but Shannon's formula for the entropy or information of a source is a dimensionless quantity (unless we assert that the bit itself is a dimension). Mathematically, Shannon's entropy is merely a parameter of a probability distribution. If Shannon himself, in his original 1948 paper, had not observed the resemblance between his expression for information and the formula for entropy in thermodynamics (where entropy is *not* dimensionless), there would probably be far less effort spent on trying to show that information bits are *physical*. After all, every "reasonable" probability distribution has a *mean* and a *variance*, and the variance of a communication signal is called *noise*, which we think of as a physical quantity. But if we called the variance of every distribution (such as students' grades on a quiz) *noise*, would that make *variance* a physical quantity in all contexts? Again, John Wheeler leads the camp that thinks of information bits as physical and is quoted as saying, "Every physical quantity, every **it**, derives its ultimate significance from **bits**." This has led to the catch phrase "It from bit", also attributed to John Wheeler.

Perhaps it is too restrictive to require that to be considered "physical", a phenomenon must be expressible in standard units of length, mass, and time. *Cycles* are not described in cgs units, but **cycles per second** (*hertz*) are the basic unit of *frequency*, generally regarded as a physical quantity. Similarly, **bits per second** (*baud*) are the basic unit of electronic communication, but in this context the **bit** is merely John Tukey's **bit**, the binary symbol usually denoted by 0 or 1, and not specifically Shannon's **bit**, the unit of information.

Siegfried describes in considerable detail the history of thinking about quantum computing, which was suggested as a possibility for significantly improved computation as early as 1985 by David Deutsch (an advocate of the "many worlds" interpretation of quantum mechanics). But the interest intensified in 1994, when Peter Shor of Bell Labs showed how quantum computing could dramatically speed up the prime factorization of very large numbers. If implementable, this would be the death knell for the RSA algorithm invented by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977. This algorithm is widely used for cryptographic security and is the best-known system for "public key cryptography". I believe that Siegfried exaggerates the amount of reliance by governments on RSA-type systems for their secure communication of diplomatic and military messages. Even ignoring the vulnerability to quantum computing, *factorization* has never been proved to be computationally difficult. (It has not been shown to increase exponentially in difficulty with the number of digits, nor even to belong to the class of "NP-complete" problems, which are generally *believed* to be "hard".) Since the advent of the RSA algorithm, interest in factorization has increased significantly and better methods are frequently being discovered. Combined with improvements in the speed of conventional computers, the number of digits required for a number to resist an attempt at unauthorized factorization has been steadily increasing. Neither the DES (data encryption standard) promulgated by the U.S. government in 1977 nor its successor, the AES (advanced encryption standard) of 2001, is based on the difficulty of factorization. However, the RSA algorithm and several of its close relatives are widely used commercially to provide cryptographic security.

The terminology of information theory and coding has been widely adopted in describing the transmission and processing of genetic information, which is encoded in the DNA as sequences of the four symbols (called bases or nucleotides): A (adenine), C (cytosine), G (guanine), and T (thymine). Three consecutive symbols form a codeword (called a *codon*) to specify one of the twenty amino acids that form the building blocks of proteins. (A given amino acid may have as few as one or as many as six different codons which specify it.) The famous structure of DNA as a double helix, discovered in 1953 by James Watson and Francis H. C. Crick, involves a pairing of nucleotides between the two strands: A with T, and C with G, which are attracted to each other by a chemical affinity. Each strand of DNA serves as a template for making its complementary strand, and when a biological cell divides, the DNA helices uncoil, with one of the two strands going to each of the daughter cells, where a new complementary strand is then formed.

This chemical affinity between base pairs in DNA was used by Adleman (the "A" in the RSA algorithm) to demonstrate "biological computing". The *traveling salesman problem* asks for the shortest path in a graph that visits each member of a prescribed set of vertices and belongs to the class of difficult problems called "NP-complete". Adleman demonstrated a solution, in the case of a six-node graph, which required DNA nucleotides to find each other and link up in a chemical solution. While it may not be practical to scale up this example to problems that would be difficult on a conventional electronic computer, the principle was established that individual molecules can be used as computational elements.

Between DNA and protein an intermediate role is played by RNA, which is single-stranded and uses a closely related four-symbol alphabet of A, C, G, and U, where U (uracil) replaces the T (thymine) of DNA. The system whereby DNA makes RNA and RNA makes protein is the biological example that most closely resembles a "computational process" as we normally understand the term. In comparison, how the liver collects and processes its input of chemical information to determine its output of secretions would be difficult (if not impossible) to model accurately on the largest computers in existence today.

Much attention and effort have been devoted to trying to model individual neurons, specific sensory systems (such as vision, or hearing, or smell), or the entire brain and central nervous system. A large part of this effort is subsumed under the rubric of "computational neurobiology". In the chapter titled "The Computational Brain", Siegfried quotes neuroscientist Terrence Sejnowski of the Salk Institute as saying, "Things that we thought were very difficult and incredibly intellectual—like playing chess or medical diagnosis—can now be done on your PC with simple programs, whereas something as simple as walking and chewing gum at the same time is something that nobody has written a program for."

Many interesting things have been done with neural networks, especially in pattern recognition, which no deterministic program is good at. Still, the most advanced neural network, which is trivial in both complexity and capability compared to the brain of an insect, is a realistic model neither of how biological brains are structured nor of how they process information.

In his chapter on "Consciousness and Complexity", Siegfried mentions several people who have recently written on the nature of consciousness, such as the British mathematician/physicist Roger Penrose, who "believes that consciousness has something to do with quantum effects in microtubules…." Siegfried adds, "I've discussed his conclusions with prominent computer scientists, neuroscientists, and quantum physicists and have yet to find anyone from these specialties who thinks Penrose is on target.… In any case, there doesn't seem to be the slightest shred of evidence for any of Penrose's conclusions."

Since there is no precise or generally agreed-upon definition of just what consciousness is, speculations about it seem, to this reviewer, to be the modern continuation of the medieval debates about the nature of the soul rather than a contribution to "hard" science. Even the experiments aimed at locating the areas in the brain associated with "consciousness" are merely detecting awareness of stimuli, a component of consciousness to be sure, but one that is widespread throughout much of the animal kingdom.

Siegfried comments that, since "brain imaging technologies have made it possible to peer inside the skull without a scalpel…philosophers and scientists alike have consumed a lot of ink in attempting to explain consciousness." He then quotes Francis Crick as saying that "there are too many people talking about it and not much doing." A paper by Crick and Christof Koch quotes from a hotel menu: "When all is said and done, more is said than done." This is an apt comment regarding the present state of pontificating about "consciousness".

Although it has little to do with information bits and computing, Siegfried could not resist the temptation to describe the current state of superstring theory, mentioned as the most promising attempt so far to unify general relativity and quantum mechanics. He mentions that *M-branes*, a recent wrinkle, require an eleven-dimensional universe (rather than the earlier ten dimensions) and offer the possibility that measurements of gravity at submillimeter distances might actually make superstring theory testable in the near future. However, it is also very possible that this theory will remain untestable for decades, or even centuries, to come.

Although *The Bit and the Pendulum* is completely devoid of equations, the scientific concepts it presents are accurately described, and the writing is enjoyable to read. The sweep of the book is impressive, and even the well-informed mathematician or scientist is likely to learn interesting things outside his/her own areas of specialization. The speculative ideas presented are indicated as such and identified with their originators. Views that have gained few reputable adherents or that have gone out of favor are, when presented, appropriately stigmatized. Of course, the reader must remember that the popularization is not the physical theory when that theory is properly described only by its equations, and a scientific theory is only as good as its predictions. Some of the areas described, such as research about consciousness, have not yet reached the stage where they make any meaningful predictions, while others, such as superstring theory, while very elegant mathematically, may not be testable for the foreseeable future. A very useful feature of this book is a six-page bibliography for "Further Reading", organized according to the topics in the introduction and the twelve chapters. The seven-page index lists the concepts and all the people mentioned in the text.