August 21, 2014

A review of Scott Aaronson's "Quantum Computing Since Democritus"

Avi Wigderson, IAS

Before turning to the book itself, let me start with a short introduction to Quantum Computing.

Quantum computing is one of the most exciting, rapidly developing scientific fields in the intersection of computer science and physics. It started from the idea, proposed independently by Richard Feynman and Yuri Manin in the early 1980s, that we might enhance the power of "classical" computers, which we all have on our laps, by letting them take advantage of quantum mechanical effects. For Feynman this was a natural suggestion — he observed that classical computers take an exponentially long time to simulate many-particle quantum systems, and if this slowdown is inherent, perhaps quantum mechanical computers can give us exponential speed-ups for important computational problems.

A formal model of computation (called a Quantum Turing Machine) capturing this idea was developed in the 1990s, and a theoretical study commenced to see what problems it could solve efficiently (if we could build one). Shortly thereafter Peter Shor discovered his famous quantum factoring algorithm, which allows such a model to factor integers exponentially faster than the best classical algorithm we know. Recall that it is the *assumed* exponential hardness of integer factoring which underlies the universal trust in the RSA crypto system and hence most security and electronic commerce applications. Thus, Shor's algorithm sent a shocking message: if anyone had a quantum computer, it could break in seconds the most sophisticated codes used by governments, armies, banks, and Amazon shoppers.

This had an immediate effect. Governments and industry began to invest billions in developing the necessary technology to build quantum computers. It should be stressed that as far as we know, there is no theoretical obstacle to building them. Nevertheless, progress has been extremely slow, at least if you take factoring as a yardstick — the largest number which a current quantum computer can factor is 21. The jury is still out on the feasibility of large-scale quantum computers, and whether unfeasibility should be blamed on technological barriers or incompleteness of quantum mechanics (e.g. perhaps it should be revised when the number of particles is really large, just as Newtonian mechanics needed revision at very large speeds or very small scales). However, the theoretical study of this subject took off as well, with a remarkably fruitful interaction (or should I say, constructive interference) between computer scientists and physicists, whose range is constantly expanding with insights from both sides. Even if we don't have general purpose quantum computers, we have already expanded considerably our understanding of, among others, quantum information theory, quantum cryptography, quantum Hamiltonian dynamics, classical computational complexity theory, the nature of randomness, and basic issues at the heart of the philosophy of science, including whether quantum mechanics itself is a falsifiable theory. In short, quantum computing is pretty irresistible!

Now to the book itself, which I greatly enjoyed reading.

This book is unique! Like its author, it is erratic, deep, funny, intellectual, juvenile, curious, honest, observant, and I am sure if you read the book you will come up with additional relevant adjectives of your own. It is not for everyone, but I guarantee that there is much insight, wisdom, and fun in these pages to amply reward those who'll put in the individually required effort (possibly to fill in some blanks, or stomach the style, depending on your knowledge and taste). Now let me elaborate on the efforts, rewards and the character of the book.

See, the book is not really about quantum computing. It is far broader, and uses quantum computing as an opportunity to introduce a whole set of important concepts in math, physics, philosophy, and, above all, computational complexity theory. This emphasis is natural and important. Computational complexity, which like the author's is my intellectual home, has undergone a tremendous expansion during the past few decades. It started as the quest to understand efficient computation — what are the best algorithms to solve natural computational tasks on a variety of computational models, where "best" can be measured by different computational resources like time, memory, energy, etc. It then evolved to inspect, through the computational lens, fundamental notions which humanity has been studying and debating for millennia, including proof, knowledge, learning, randomness, and more, often revealing new properties and notions of these central issues. It also started modeling and analyzing algorithms which nature uses to "solve its own problems", namely run the universe. After all, so many natural processes can be viewed as information processes, and the know-how of the field, initially designed for computer algorithms, naturally suits their study. The result was a web of interactions among many scientific disciplines.

The author uses quantum computing, his speciality and passion, as a focal point through which to expose this broad intellectual adventure. You will learn about the origins of the theory of computation, with logic, set theory, and the crisis in the foundations of mathematics. You will learn the rudiments of computational complexity theory and its *methodology*, how algorithms are analyzed, the P versus NP problem, how problems are classified into complexity classes, reduction and completeness. You'll see the ease with which quantum computing, just like a host of other types of computing, fits this framework and starts interacting with other parts of this field. Then you will learn about new computational definitions and meanings of the notions above, proofs, secrets, pseudo-random generators, and indeed learning. You will see how they all fit the methodology, are intimately related to each other and to computational difficulty, and how they adapt to the appearance of quantum mechanics in the computational model. This understanding turns out to have great impact on both physics and computation! The book's ambition is to show you all these wonders and more.

The reader may be surprised at how little quantum mechanics is presented or needed. This is another part of the beauty here. To understand quantum computing, all you need are the basic principles of quantum mechanics — unitary evolution, linearity and the notion of measurement. The author points out that this "extension of probability theory" which works in the 2-norm and with complex numbers, is a much better introduction to quantum mechanics than the standard one found in most textbooks. This mathematical setting already explains most of the paradoxes and subtle issues raised by this strange theory, many of which, like the Bell inequalities, the uncertainty principle, and interpretations of quantum mechanics are treated in the book.

Finally, the book discusses a host of philosophical issues, related and unrelated to the main topic. These include free will, time travel, the anthropic principle, the questions of whether our brains are machines, and much more, as well as an arsenal of paradoxes. All are handled with clarity, seeing to the heart of things and clearing the typical smoke screens of ambiguity, and with professional honesty that does not shy away from pointing out nonsense, even when articulated by famous people.

So far so good. So why did I warn you in the beginning that the book is not for everyone, and that I expect the typical reader, even an expert scientist or mathematician, to need to invest effort when reading the book? Well, the author himself supplies some reasons in his opening pre-preface "critical review" of his book. With characteristic professional honesty he tells the reader, among other things:

"Yes it's hard to avoid the suspicion that Quantum Computing Since Democritus *is basically a 'brain dump': a collection of thoughts about theoretical computer science, physics, math, and philosophy that were on the author's mind around 2006, when he gave a series of lectures at the university of Waterloo that eventually turned into this book. The material is tied together by the author's nerdy humor, his 'Socratic' approach to every question, and his obsession with the theory of computation and how it relates to the physical world."*

The author goes on to speculate about who might be potential readers of this book, which is neither "popular" nor a "textbook". And I agree that all types discussed (colleagues, engineers, programmers, scientists, mathematicians, highly motivated high school students, laymen who read science blogs), will all potentially benefit greatly if they manage to actually cover significant parts of the book. So what can make reading the book difficult? I expect that not all will like the writing style. Some may find the many (splendid) diversions from the main course too distracting. But the main hurdle I believe is that, as the book is very broad, it necessarily skips over lots of background material that would make the book easier to read. This was probably not a major issue for those attending the lectures on which the book is based; most were motivated students who had already taken a variety of related courses on the various topics covered, and those who had not could check with the professor or their friends to find out how to fill the gaps. One cannot assume that book's readers have the same convenience. Of course, the material and its organization and presentation are the author's to choose. But I wish the book had supplied specific references to high-quality sources, like surveys and books that the author recommends (as opposed to saying that it can be found e.g. "in dozens of textbooks"). On a related note, extremely few references to original works are given and many major ones are missing—a set of bibliographic notes at the end of each chapter would have been welcome (perhaps we'll see it in the 2nd edition).

To conclude, let me remind you of my main recommendation. The shortcomings mentioned above pale in comparison to the value of this book. So read it, investing what you need to keep going. You will be rewarded by the wealth of knowledge, by seeing the power of computational thinking, and by experiencing the diversity of the deeply intellectual, fun activities in the vast playground laid out so uniquely by the author.