

QUANTUM COMPUTING SINCE DEMOCRITUS



SCOTT AARONSON

Quantum Computing since Democritus

Written by noted quantum computing theorist Scott Aaronson, this book takes readers on a tour through some of the deepest ideas of math, computer science, and physics.

Full of insights, arguments, and philosophical perspectives, the book covers an amazing array of topics. Beginning in antiquity with Democritus, it progresses through logic and set theory, computability and complexity theory, quantum computing, cryptography, the information content of quantum states, and the interpretation of quantum mechanics. There are also extended discussions about time travel, Newcomb's Paradox, the Anthropic Principle, and the views of Roger Penrose. Aaronson's informal style makes this fascinating book accessible to readers with scientific backgrounds, as well as students and researchers working in physics, computer science, mathematics, and philosophy.

SCOTT AARONSON is an Associate Professor of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology. Considered one of the top quantum complexity theorists in the world, he is well known both for his research in quantum computing and computational complexity theory, and for his widely read blog *Shtetl-Optimized*. Professor Aaronson also created Complexity Zoo, an online encyclopedia of computational complexity theory, and has written popular articles for *Scientific American* and *The New York Times*. His research and popular writing have earned him numerous awards, including the United States Presidential Early Career Award for Scientists and Engineers and the Alan T. Waterman Award.

Quantum Computing since Democritus

SCOTT AARONSON

Massachusetts Institute of Technology



CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town,
Singapore, São Paulo, Delhi, Mexico City

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK
Published in the United States of America by Cambridge University Press,
New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521199568

© S. Aaronson 2013

This publication is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without the written
permission of Cambridge University Press.

First published 2013

Printed and bound in the United Kingdom by the MPG Books Group

A catalog record for this publication is available from the British Library

Library of Congress Cataloging in Publication data

Aaronson, Scott.

Quantum computing since Democritus / Scott Aaronson.

pages cm

Includes bibliographical references and index.

ISBN 978-0-521-19956-8 (pbk.)

1. Quantum theory – Mathematics. 2. Quantum computers. I. Title.

QC174.17.M35A27 2013

621.39'1 – dc23 2012036798

ISBN 978-0-521-19956-8 Paperback

Cambridge University Press has no responsibility for the persistence or
accuracy of URLs for external or third-party internet websites referred to
in this publication, and does not guarantee that any content on such
websites is, or will remain, accurate or appropriate.

To my parents

Contents

| | |
|--------------------------------------|----------------|
| Preface | <i>page ix</i> |
| Acknowledgments | <i>xxix</i> |
| 1. Atoms and the void | 1 |
| 2. Sets | 8 |
| 3. Gödel, Turing, and friends | 18 |
| 4. Minds and machines | 29 |
| 5. Paleocomplexity | 44 |
| 6. P, NP, and friends | 54 |
| 7. Randomness | 71 |
| 8. Crypto | 93 |
| 9. Quantum | 109 |
| 10. Quantum computing | 132 |
| 11. Penrose | 150 |
| 12. Decoherence and hidden variables | 160 |
| 13. Proofs | 186 |

| | |
|--|-----|
| 14. How big are quantum states? | 200 |
| 15. Skepticism of quantum computing | 217 |
| 16. Learning | 228 |
| 17. Interactive proofs, circuit lower bounds, and more | 243 |
| 18. Fun with the Anthropic Principle | 266 |
| 19. Free will | 290 |
| 20. Time travel | 307 |
| 21. Cosmology and complexity | 325 |
| 22. Ask me anything | 343 |
| Index | 363 |

Preface

A CRITICAL REVIEW OF SCOTT AARONSON'S
QUANTUM COMPUTING SINCE DEMOCRITUS

by Scott Aaronson.

Quantum Computing since Democritus is a candidate for the weirdest book ever to be published by Cambridge University Press. The strangeness starts with the title, which conspicuously fails to explain what this book is *about*. Is this another textbook on quantum computing – the fashionable field at the intersection of physics, math, and computer science that's been promising the world a new kind of computer for two decades, but has yet to build an actual device that can do anything more impressive than factor 21 into 3×7 (with high probability)? If so, then what does *this* book add to the dozens of others that have already mapped out the fundamentals of quantum computing theory? Is the book, instead, a quixotic attempt to connect quantum computing to ancient history? But what does Democritus, the Greek atomist philosopher, really have to do with the book's content, at least half of which would have been new to scientists of the 1970s, let alone of 300 BC?

Having now read the book, I confess that I've had my mind blown, my worldview reshaped, by the author's truly brilliant, original perspectives on everything from quantum computing (as promised in the title) to Gödel's and Turing's theorems to the **P** versus **NP** question to the interpretation of quantum mechanics to artificial intelligence to Newcomb's Paradox to the black-hole information loss problem. So, if anyone were perusing this book at a bookstore, or with Amazon's "Look Inside" feature, I would *certainly* tell that person to buy a copy immediately. I'd also add that the author is extremely handsome.

Yet 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 the fall of 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. But if there's some overarching "thesis" that I'm supposed to take away, I can't for the life of me articulate what it is.

More pointedly, one wonders who the *audience* for this book is supposed to be. On the one hand, it has *way* too much depth for a popular book. Like Roger Penrose's *The Road to Reality* – whose preface promises an accessible adventure even for readers who struggled with fractions in elementary school, but whose first few chapters then delve into holomorphic functions and fiber bundles – *Quantum Computing since Democritus* is not for math-phobes. A curious layperson could *certainly* learn a lot from this book, but he or she would have to be willing to skip over some dense passages, possibly to return to them later. So if you're someone who can stomach "science writing" only after it's been carefully cleansed of the science, look elsewhere.

On the other hand, the book is *also* too wide-ranging, breezy, and idiosyncratic to be used much as a textbook or reference work. Sure, it has theorems, proofs, and exercises, and it covers the basics of an astonishing number of fields: logic, set theory, computability, complexity, cryptography, quantum information, and computational learning theory, among others. It seems likely that students in any of those fields, from the undergraduate level on up, could gain valuable insights from this book, or could use it as an entertaining self-study or refresher course. Besides these basics, the book also has significant material on quantum complexity theory – for example, on the power of quantum proofs and advice – that (to this reviewer's knowledge)

hasn't appeared anywhere else in book form. But still, the book flits from topic to topic too hastily to be a definitive text on anything.

So, is the book aimed at non-scientists who won't *actually* make it past the first chapter, but want something to put on their coffee table to impress party guests? The only other possibility I can think of is that there's an underserved audience for science books that are neither "popular" nor "professional": books that describe a piece of the intellectual landscape from one researcher's heavily biased vantage point, using the same sort of language you might hear in a hallway conversation with a colleague from a different field. Maybe, besides those colleagues, this hypothetical "underserved audience" would include precocious high-school students, or programmers and engineers who enjoyed their theoretical courses back in college and want to find out what's new. Maybe this is the same audience that frequents these "science blogs" I've heard about: online venues where anyone in the world can apparently watch real scientists, people at the forefront of human knowledge, engage in petty spats, name-calling, and every other juvenile behavior, and can even egg the scientists on to embarrass themselves further. (The book's author, it should be noted, writes a particularly crass and infamous such blog.) *If* such an audience actually exists, then perhaps the author knew exactly what he was doing in aiming at it. My sense, though, is that he was having too much fun to be guided by any such conscious plan.

NOW FOR THE ACTUAL PREFACE

While I appreciate the reviewer's kind words about my book (and even my appearance!) in the preceding pages, I also take issue, in the strongest possible terms, with his ignorant claim that *Quantum Computing since Democritus* has no overarching thesis. It *does* have a thesis – even though, strangely, I wasn't the one who figured out what it was. For identifying the central message of this book, I need to thank Love Communications, an advertising agency based in

Sydney, Australia, which put the message into the mouths of fashion models for the purpose of selling printers.

Let me explain – the story is worth it.

In 2006, I taught a course entitled “Quantum Computing since Democritus” at the University of Waterloo. Over the next year, I posted rough notes from the course on my blog, *Shtetl-Optimized*¹ – notes that were eventually to become this book. I was heartened by the enthusiastic response from readers of my blog; indeed, that response is what convinced me to publish this book in the first place. But there was one response neither I nor anyone else could have predicted.

On October 1, 2007, I received an email from one Warren Smith in Australia, who said he had seen a television commercial for Ricoh printers. The commercial, he went on, featured two female fashion models in a makeup room, having the following conversation:

Model 1: But if quantum mechanics isn’t physics in the usual sense – if it’s not about matter, or energy, or waves – then what *is* it about?

Model 2: Well, from my perspective, it’s about information, probabilities, and observables, and how they relate to each other.

Model 1: That’s interesting!

The commercial then flashed the tagline “A more intelligent model,” followed by a picture of a Ricoh printer.

Smith said he was curious where the unusual text had come from, so he googled it. Doing so brought him to Chapter 9 of my “Quantum Computing since Democritus” notes (p. 110), where he found the following passage:

But if quantum mechanics isn’t physics in the usual sense – if it’s not about matter, or energy, or waves, or particles – then what *is* it

¹ www.scottaaronson.com/blog

about? From my perspective, it's about information and probabilities and observables, and how they relate to each other.

So, it seemed, there was exactly one bit of dialogue in the commercial that I *didn't* write ("That's interesting!"). Smith found a link² where I could see the commercial for myself on YouTube, and his story checked out.

Far more amused than annoyed, I wrote a post for my blog, entitled "Australian Actresses Are Plagiarizing My Quantum Mechanics Lecture to Sell Printers."³ After relating what had happened and linking to the video, the post ended

For almost the first time in my life, I'm at a loss for words. I don't know how to respond. I don't know which of 500 000 possible jokes to make. Help me, readers. Should I be flattered? Should I be calling a lawyer?

This would become the most notorious blog post I ever wrote. By the next morning, the story had made the *Sydney Morning Herald* ("Ad agency cribbed my lecture notes: professor"⁴), Slashdot ("Scott Aaronson, Printer Shill"⁵), and several other news sites. I happened to be in Latvia at the time, visiting my colleague Andris Ambainis, but somehow journalists tracked me down to my hotel room in Riga, waking me up around 5 a.m. to ask for interviews.

Meanwhile, reactions on my blog and in other online forums were mixed. Some readers said I'd be foolish if I didn't sue the ad agency for all it was worth. What if they had played a few beats of a *Rolling Stones* song, without first getting permission? Cases like that, I was assured, are sometimes settled for millions of dollars. Others said that even *asking the question* made me a stereotypical litigious American, a personification of everything wrong with the world. I should be flattered, they continued, that the ad writers had

² www.youtube.com/watch?v=saWCyZupO4U

³ www.scottaaronson.com/blog/?p=277

⁴ www.smh.com.au/news/technology/professor-claims-ad-agency-cribs-lecture-notes/2007/10/03/1191091161163.html

⁵ idle slashdot.org/story/07/10/02/1310222/scott-aaronson-printer-shill

seen fit to give *my* take on quantum mechanics all this free publicity. Dozens of commenters offered variations on the same insipid joke, that I should ask for a date with the “models” as my compensation. (I replied that I’d rather have a free printer, if it came down to it.) One commenter simply wrote, “This really could be the funniest thing that has ever happened.”

For its part, Love Communications admitted that it had appropriated material from my lecture, but said it had consulted a lawyer and thought it was perfectly within its fair-use rights to do so. Meanwhile, I *did* get in touch with an Australian intellectual property lawyer, who said that I might have a case – but it would take time and energy to pursue it. I felt torn: on the one hand, plagiarism is one of the academic world’s few unforgivable sins, and I was miffed by the agency’s completely unapologetic response, after they’d been caught so red handed. On the other hand, if they had just *asked* me, I probably would have gladly given them permission to use my words, for either a token sum or no money at all.

In the end, we found a solution that everyone liked. Love Communications apologized (without admitting wrongdoing), and donated \$5000 to two science outreach organizations of my choice in Australia.⁶ In return, I didn’t pursue any further action – and indeed, I mostly forgot about the affair, except when colleagues would rib me (as they continue to do) about Australian models.

But there’s a final irony to the tale, and that’s why I’m recounting it here (well, besides just that it’s a hilarious true story involving this book). If I had to choose one passage from the entire book to be broadcast on TV, I think I would have chosen the exact same one that the commercial writers chose – even though they were presumably just trawling for some sciencey-sounding gobbledygook, and I hadn’t highlighted the passage in any way, as its centrality hadn’t occurred to me.

⁶ See www.scottaaronson.com/blog/?p=297

The idea that quantum mechanics is “about” information, probabilities, and observables, rather than waves and particles, certainly isn’t an original one. The physicist John Archibald Wheeler said similar things in the 1970s; and today an entire field, that of quantum computing and information, is built around the idea. Indeed, in the discussion on my blog that followed the Australian models episode, one the commonest (and to me, funniest) arguments was that I had no right to complain, because the appropriated passage *wasn’t special in any way*: it was an obvious thought that could be found in any physics book!

How I wish it were so. Even in 2013, the view of quantum mechanics as a theory of information and probabilities remains very much a minority one. Pick up almost any physics book – whether popular or technical – and you’ll learn that (a) modern physics says all sorts of paradoxical-seeming things, like that waves are particles and particles are waves, (b) at a deep level, no one really understands these things, (c) even translating them into math requires years of intensive study, but (d) they make the atomic spectra come out right, and that’s what matters in the end.

One eloquent statement of this “conventional view” was provided by Carl Sagan, in *The Demon-Haunted World*:

Imagine you seriously want to understand what quantum mechanics is about. There is a mathematical underpinning that you must first acquire, mastery of each mathematical subdiscipline leading you to the threshold of the next. In turn you must learn arithmetic, Euclidean geometry, high school algebra, differential and integral calculus, ordinary and partial differential equations, vector calculus, certain special functions of mathematical physics, matrix algebra, and group theory . . . The job of the popularizer of science, trying to get across some idea of quantum mechanics to a general audience that has not gone through these initiation rites, is daunting. Indeed, there are no successful popularizations of quantum mechanics in my opinion – partly for this reason. These

mathematical complexities are compounded by the fact that quantum theory is so resolutely counterintuitive. Common sense is almost useless in approaching it. It's no good, Richard Feynman once said, asking why it *is* that way. No one knows why it is that way. That's just the way it is (p. 249).

It's understandable why physicists talk this way: because physics is an experimental science. In physics you're *allowed* to say, "these are the rules, not because they make sense, but because we ran the experiment and got such-and-such a result." You can even say it proudly, gleefully – *defying* the skeptics to put their preconceived notions up against Nature's verdict.

Personally, I simply *believe* the experimentalists, when they say the world works in a completely different way than I thought it did. It's not a matter of convincing me. Nor do I presume to predict what the experimentalists will discover next. All I want to know is: *What went wrong with my intuition? How should I fix it, to put it more in line with what the experiments found? How could I have reasoned, such that the actual behavior of the world **wouldn't** have surprised me so much?*

With several previous scientific revolutions – Newtonian physics, Darwinian evolution, special relativity – I feel like I more-or-less know the answers to the above questions. If my intuition isn't yet fully adjusted even to those theories, then at least I know how it *needs* to be adjusted. And thus, for example, if I were creating a new universe, I might or might not decide to make it Lorentz invariant, but I'd certainly *consider* the option, and I'd understand why Lorentz-invariance was the inevitable consequence of a couple of other properties I might want.

But quantum mechanics is different. Here, the physicists assure us, *no one knows* how we should adjust our intuition so that the behavior of subatomic particles would no longer seem so crazy. Indeed, maybe there *is* no way; maybe subatomic behavior will always remain an arbitrary brute fact, with nothing to say about it

beyond “such-and-such formulas give you the right answer.” My response is radical: if that’s true, then *I don’t much care* how subatomic particles behave. No doubt other people *need* to know – the people designing lasers or transistors, for example – so let them learn. As for me, I’ll simply study another subject that makes more sense to me – like, say, theoretical computer science. Telling me that my physical intuition was wrong, without giving me any path to *correct* that intuition, is like flunking me on an exam without providing any hint about how I could’ve done better. As soon as I’m free to do so, I’ll simply gravitate to other courses where I get As, where my intuition *does* work.

Fortunately, I think that, as the result of decades of work in quantum computation and quantum foundations, we *can* do a lot better today than simply calling quantum mechanics a mysterious brute fact. To spill the beans, here’s the perspective of this book:

Quantum mechanics is a beautiful generalization of the laws of probability: a generalization based on the 2-norm rather than the 1-norm, and on complex numbers rather than nonnegative real numbers. It can be studied completely separately from its applications to physics (and indeed, doing so provides a good starting point for learning the physical applications later). This generalized probability theory leads naturally to a new model of computation – the quantum computing model – that challenges ideas about computation once considered a priori, and that theoretical computer scientists might have been driven to invent for their own purposes, even if there were no relation to physics. In short, while quantum mechanics was invented a century ago to solve technical problems in physics, today it can be fruitfully explained from an extremely different perspective: as part of the history of ideas, in math, logic, computation, and philosophy, about the limits of the knowable.

In this book I try to make good on the above claims, taking a leisurely and winding route to do so. I start, in Chapter 1, as near to

the “beginning” as I possibly can: with Democritus, the ancient Greek philosopher. Democritus’s surviving fragments – which speculate, among other things, that all natural phenomena arise from complicated interactions between a few kinds of tiny “atoms,” whizzing around in mostly empty space – get closer to a modern scientific worldview than anything else in antiquity (and certainly closer than any of Plato’s or Aristotle’s ideas). Yet no sooner had Democritus formulated the atomist hypothesis, than he noticed uneasily its tendency to “swallow whole” the very sense-experiences that he was presumably trying to explain in the first place. How could *those* be reduced to the motions of atoms? Democritus expressed the dilemma in the form of a dialogue between the Intellect and the Senses:

Intellect: By convention there is sweetness, by convention bitterness, by convention color, in reality only atoms and the void.

Senses: Foolish intellect! Do you seek to overthrow us, while it is from us that you take your evidence?

This two-line dialogue will serve as a sort of touchstone for the entire book. One of my themes will be how quantum mechanics seems to give both the Intellect *and* the Senses unexpected new weapons in their 2300-year-old argument – while still (I think) not producing a clear victory for either.

In Chapters 2 and 3, I move on to discuss the deepest knowledge we have that intentionally *doesn’t* depend on “brute facts” about the physical world: namely, mathematics. Even there, something inside me (and, I suspect, inside many other computer scientists!) is suspicious of those *parts* of mathematics that bear the obvious imprint of physics, such as partial differential equations, differential geometry, Lie groups, or anything else that’s “too continuous.” So instead, I start with some of the most “physics-free” parts of math yet discovered: set theory, logic, and computability. I discuss the great discoveries of Cantor, Frege,

Gödel, Turing, Church, and Cohen, which helped to map the contours of mathematical reasoning itself – and which, in the course of showing why all of mathematics can't be reduced to a fixed "mechanical process," also demonstrated just how much of it *could* be, and clarified what we mean by "mechanical process" in the first place. Since I can't resist, in Chapter 4 I then wade into the hoary debate about whether the human mind, too, is governed by "fixed mechanical processes." I set out the various positions as fairly as I can (but no doubt reveal my biases).

Chapter 5 introduces computability theory's modern cousin, *computational complexity theory*, which plays a central role in the rest of the book. I try to illustrate, in particular, how computational complexity lets us systematically take "deep philosophical mysteries" about the limits of knowledge, and convert them into "merely" insanely difficult unsolved mathematical problems, which arguably capture most of what we want to know! There's no better example of such a conversion than the **P** versus **NP** problem, which I discuss in Chapter 6. Then, as warmups to quantum computing, Chapter 7 examines the many uses of *classical* randomness, both in computational complexity and in other parts of life; and Chapter 8 explains how computational complexity ideas were applied to revolutionize the theory and practice of *cryptology* beginning in the 1970s.

All of that is just to set the stage for the most notorious part of the book: Chapter 9, which presents my view of quantum mechanics as a "generalized probability theory." Then Chapter 10 explains the basics of my own field, the *quantum theory of computation*, which can be briefly defined as the merger of quantum mechanics with computational complexity theory. As a "reward" for persevering through all this technical material, Chapter 11 offers a critical examination of the ideas of Sir Roger Penrose, who famously holds that the brain is not merely a quantum computer but quantum *gravitational* computer, able to solve Turing-uncomputable problems – and that this, or something like it, can be shown by an

appeal to Gödel's Incompleteness Theorem. It's child's play to point out the problems with these ideas, and I do so, but what I find more interesting is to ask whether there *might* be nuggets of truth in Penrose's speculations. Then Chapter 12 confronts what I see as the central conceptual problem of quantum mechanics: not that the future is indeterminate (who cares?!), but that the past is *also* indeterminate! I examine two very different responses to that problem: first, the appeal, popular among physicists, to *decoherence*, and to the "effective arrow of time" supplied by the Second Law of Thermodynamics; and second, "hidden-variable theories" such as Bohmian mechanics. Even if hidden-variable theories are rejected, I find that they lead to some extremely interesting mathematical questions.

The rest of the book consists of applications of the perspective developed earlier, to various big, exciting, or controversial questions in math, computer science, philosophy, and physics. Much more than the earlier chapters, the later ones discuss *recent research* – mostly in quantum information and computational complexity, but also a bit in quantum gravity and cosmology – that strikes me as having some hope of shedding light on these "big questions." As such, I expect that the last chapters will be the first to become outdated! While there are minor dependencies, to a first approximation the later chapters can be read in any order.

- Chapter 13 discusses new notions of mathematical proof (including probabilistic and zero-knowledge proofs), then applies those notions to understanding the computational complexity of hidden-variable theories.
- Chapter 14 takes up the question of the "size" of quantum states – do they encode an exponential amount of classical information, or not? – and relates this question to the quantum interpretation debate on the one hand, and to recent complexity-theoretic research on quantum proofs and advice on the other.
- Chapter 15 examines the arguments of quantum computing *skeptics*: the people who hold, not merely that building a practical quantum

computer is hard (which everyone agrees about!), but that it can *never be done* for some fundamental reason.

- Chapter 16 examines Hume's Problem of Induction, using it as a jumping-off point for discussing *computational learning theory*, as well as recent work on the learnability of quantum states.
- Chapter 17 discusses some breakthroughs in our understanding of classical and quantum *interactive proof systems* (e.g., the **IP = PSPACE** and **QIP = PSPACE** theorems), but is mostly interested in those breakthroughs insofar as they've led to *non-relativizing circuit lower bounds* – and, therefore, might illuminate something about the **P** versus **NP** question.
- Chapter 18 examines the famous Anthropic Principle and “Doomsday Argument”; the discussion starts out highly philosophical (of course), but eventually winds its way to a discussion of *postselected quantum computing* and the **PostBQP = PP** theorem.
- Chapter 19 discusses Newcomb's Paradox and free will, leading into an account of the Conway–Kochen “free will theorem,” and the use of Bell's Inequality to generate “Einstein-certified random numbers.”
- Chapter 20 takes up time travel: in a now-familiar pattern, starting with a wide-ranging philosophical discussion, and ending with a proof that classical or quantum computers with closed timelike curves yield exactly the computational power of **PSPACE** (under assumptions that are open to interesting objections, which I discuss at length).
- Chapter 21 discusses cosmology, dark energy, the Bekenstein bound, and the holographic principle – but, not surprisingly, with an eye toward what all these things mean for *the limits of computation*. For example, how many bits can one store or search through, and how many operations can one perform on those bits, without using so much energy that one instead creates a black hole?
- Chapter 22 is “dessert”: it's based off the final lecture of the Quantum Computing Since Democritus class, in which the students could ask me anything whatsoever, and watch me struggle to respond. Topics addressed include the following: the possible breakdown of quantum mechanics; black holes and “fuzzballs”; the relevance of oracle results in computational complexity; **NP**-complete problems and creativity;

“super-quantum” correlations; derandomization of randomized algorithms; science, religion, and the nature of rationality; and why computer science is not a branch of physics departments.

A final remark. One thing you *won't* find in this book is much discussion of the “practicalities” of quantum computing: either physical implementation, or error correction, or the details of Shor's, Grover's, or other basic quantum algorithms. One reason for this neglect is incidental: the book is based on lectures I gave at the University of Waterloo's Institute for Quantum Computing, and the students were already learning all about those aspects in their other classes. A second reason is that those aspects are covered in *dozens* of other books⁷ and online lecture notes (including some of my own), and I saw no need to reinvent the wheel. But a third reason is, frankly, that the technological prospect of building a new kind of computer, exciting as it is, is not why I went into quantum computing in the first place. (*Shhh*, please don't tell any funding agency directors I said that.)

To be clear, I think it's entirely possible that I'll see practical quantum computers in my lifetime (and also possible, of course, that I *won't* see them). And if we *do* get scalable, universal quantum computers, then they'll almost certainly find real applications (not even counting codebreaking): mostly, I think, for specialized tasks like quantum simulation, but to a lesser extent for solving combinatorial optimization problems. If that ever happens, I expect I'll be as excited about it as anyone on earth – and, of course, tickled if any of the work I've done finds applications in that new world. On the other hand, if someone gave me a practical quantum computer tomorrow, then I confess that I can't think of anything that I, personally, would want to use it for: only things that *other people* could use it for!

⁷ The “standard reference” for the field remains *Quantum Computation and Quantum Information*, by Michael Nielsen and Isaac Chuang.

sample content of Quantum Computing since Democritus

- [download online Private Empire: ExxonMobil and American Power](#)
- [download Gardening When It Counts: Growing Food in Hard Times for free](#)
- [Last Plane to Heaven: The Final Collection.pdf, azw \(kindle\)](#)
- [read online A Companion To Greek Mythology \(Blackwell Companions To The Ancient World\) for free](#)
- [read The Sexual Constitution of Political Authority: The 'Trials' of Same-Sex Desire \(Social Justice\) for free](#)
- [download Visual Tools for Transforming Information Into Knowledge for free](#)

- <http://rodrigocaporal.com/library/The-Hair-of-Harold-Roux.pdf>
- <http://econtact.webschaefer.com/?books/Gardening-When-It-Counts--Growing-Food-in-Hard-Times.pdf>
- <http://berttrotman.com/library/Guyton-and-Hall-Textbook-of-Medical-Physiology--12th-Edition-.pdf>
- <http://www.netc-bd.com/ebooks/A-Companion-To-Greek-Mythology--Blackwell-Companions-To-The-Ancient-World-.pdf>
- <http://aseasonedman.com/ebooks/16-Lighthouse-Road--Cedar-Cove--Book-1-.pdf>
- <http://cambridgebrass.com/?freebooks/Harry-Potter-y-el-prisionero-de-Azkaban.pdf>