Quantum Information and Computation, Vol. 1, No. 2 (2001) 95–96

BOOK REVIEW

on

Quantum Computation and Quantum Information

Michael A. Nielsen & Isaac L. Chuang

Cambridge Univ Press, 2000

$47.95 (675 pages) ISBN: 0521635039

In a space of less than ten years, a cadre of inspired researchers from theoretical and experimental physics, computer science, and mathematics have been incessantly at work building an entirely new body of knowledge about the information processing capabilities of quantum systems. The amount of wisdom accumulated in these short years already presses at the limits of what one mind can reasonably apprehend. But many of us have felt from the beginning that our subject possesses an underlying intellectual structure of great power and clarity, sufficient to hold and display even the weighty mass of knowledge that we have accumulated, and to provide a framework for future developments.

Nielsen and Chuang have tackled the job of drawing the blueprint of this structure. This in itself has been a Herculean task: the building is extensive, and most of it has never been mapped out before. Their plan has been rigorous and original. More than any of the previous attempts, this book has identified the essential foundations of quantum information theory with a clarity that has even, in a few cases, permitted the authors to obtain some original results and point toward new research directions.

The plan of the book weaves together topics of physical theory and information theory. Nielsen and Chuang start with basic introductions to quantum theory and to the basic elements of theoretical computer science. For the physicist, the quantum mechanics will be elementary, but it is deceptively so: for example, we get a careful discussion here of the tensor product structure of Hilbert space, a topic that is crucial to quantum information theory, but is usually barely mentioned (and then forgotten and misunderstood) in conventional quantum theory texts. The book then moves on to discuss quantum circuits and quantum algorithms, physical realizations of quantum computers, decoherence and quantum error correction, and finally quantum entropies and quantum channel theory.

This book is no mere compendium of standard results. In several instances, the authors delve very deeply into a problem, and come up with results that appear nowhere else in the literature. An example of this is their treatment of quantum gate universality. Most repertoires of quantum gates can be used to approximate, with arbitrarily high accuracy, any unitary transformation on a set of qubits. This result is known as the "Solovay-Kitaev theorem," in honor of the workers who reported (but did not entirely publish) results on this problem. The present treatment is the most complete, and certainly the most clear, treatment of the results on this problem, and has pointed towards more efficient ways to do quantum gate constructions.

Much the same can be said about the proof of security of "BB84" quantum cryptography against arbitrary eavesdropping strategies. This proof was completed some years ago by Dominic Mayers, and was recently put into a more accessible form by Shor and Preskill, building on the work of Lo and Chau. After direct and extensive interaction with Shor and Preskill, Nielsen and Chuang have fully explicated this proof for the first time in this book. I also commend their discussion of the difficult and fundamental subjects of quantum error correction and fault tolerant quantum computation as models of lucidity. The exercises and problems are very useful; the ones marked "Research" will put the student right in the thick of current activity in the field. (Perhaps some future edition will need to include solutions to some of these "Research" problems.)

The extensive scope and the considerable depth of the treatment given here will present problems for some readers and users: I expect that even the most advanced graduate course in quantum information will only be able to cover a subset of the material here. For an undergraduate course, the treatment is probably at too high a level; I expect that a useable lower-level book will only come about as the result of a completely different approach, probably by some other authors. On the other hand, despite its considerable heft, there is still room for aficionados to complain that their favorite topics in quantum information have been given short shrift in this volume: the theory of quantum entanglement is almost entirely absent, communication complexity is missing, and the new methods of quantum computing by teleportation (even those invented by one of the authors) are left out. I can only have sympathy for the authors in the hard choices that they had to make – inclusion of everything would have resulted in a three-volume set!

Some have questioned whether a book of this sort, written at such an early stage in the development of a field, will have lasting value. Surely, another ten years of progress will give the field a quite different and much enlarged look. Still, I expect that this new structure will rest well on the foundations so ably charted out in this book. This thick tome should set the standard for many years to come.

David P. DiVincenzo
IBM T. J. Watson Research Center