Computational Complexity: A Modern Approach

Draft of a book: Dated January 2007
Comments welcome!

Sanjeev Arora and Boaz Barak
Princeton University
complexitybook@gmail.com

This is an Internet draft. Some chapters are more finished than others. References and attributions are very preliminary and we apologize in advance for any omissions (but hope you will nevertheless point them out to us).

Please send us bugs, typos, missing references or general comments to
complexitybook@gmail.com — **Thank You!!**

About this book

Computational complexity theory has developed rapidly in the past three decades. The list of surprising and fundamental results proved since 1990 alone could fill a book: these include new probabilistic definitions of classical complexity classes (**IP** = **PSPACE** and the **PCP** Theorems) and their implications for the field of approximation algorithms; Shor's algorithm to factor integers using a quantum computer; an understanding of why current approaches to the famous **P** versus **NP** will not be successful; a theory of derandomization and pseudorandomness based upon computational hardness; and beautiful constructions of pseudorandom objects such as extractors and expanders.

This book aims to describe such recent achievements of complexity theory in the context of the classical results. It is intended to both serve as a textbook as a reference for self-study. This means it must simultaneously cater to many audiences, and it is carefully designed with that goal. Throughout the book we explain the context in which a certain notion is useful, and *why* things are defined in a certain way. Examples and solved exercises accompany key definitions. We assume essentially no computational background and very minimal mathematical background, which we review in Appendix A.

We have also provided a *web site* for this book at `http://www.cs.princeton.edu/theory/complexity/` with related auxiliary material. This includes web chapters on automata and computability theory, detailed teaching plans for courses based on this book, a draft of all the book's chapters, and links to other online resources covering related topics.
The book is divided into three parts:

Part I: Basic complexity classes. This volume provides a broad introduction to the field. Starting from the definition of Turing machines and the basic notions of computability theory, this volumes covers the basic time and space complexity classes, and also includes a few more modern topics such probabilistic algorithms, interactive proofs and cryptography.

Part II: Lower bounds on concrete computational models. This part describes lower bounds on resources required to solve algorithmic tasks on concrete models such as circuits, decision trees, etc. Such models may seem at first sight very different from Turing machines, but looking deeper one finds interesting interconnections.

Part III: Advanced topics. This part is largely devoted to developments since the late 1980s. It includes average case complexity, derandomization and pseudorandomness, the **PCP** theorem and hardness of approximation, proof complexity and quantum computing.

Almost every chapter in the book can be read in isolation (though we recommend reading Chapters 1, 2 and 7 before reading later chapters). This is important because the book is aimed

at many classes of readers:

- *Physicists, mathematicians, and other scientists.* This group has become increasingly interested in computational complexity theory, especially because of high-profile results such as Shor's algorithm and the recent deterministic test for primality. This intellectually sophisticated group will be able to quickly read through Part I. Progressing on to Parts II and III they can read individual chapters and find almost everything they need to understand current research.
- *Computer scientists (e.g., algorithms designers) who do not work in complexity theory per se.* They may use the book for self-study or even to teach a graduate course or seminar.
- *All those —professors or students— who do research in complexity theory or plan to do so.* They may already know Part I and use the book for Parts II and III, possibly in a seminar or reading course. The coverage of advanced topics there is detailed enough to allow this.

This book can be used as a textbook for several types of courses. We will provide several teaching plans and material for such courses on the book's web site.

- *Undergraduate Theory of Computation Course.* Part I may be suitable for an undergraduate course that is an alternative to the more traditional *Theory of Computation* course currently taught in most computer science departments (and exemplified by Sipser's excellent book with the same name [SIP96]). Such a course would have a greater emphasis on modern topics such as probabilistic algorithms and cryptography. We note that in contrast to Sipser's book, the current book has a quite minimal coverage of computability and no coverage of automata theory, but we provide web-only chapters with more coverage of these topics on the book's web site. The prerequisite mathematical background would be some comfort with mathematical proofs and elementary probability on finite sample spaces, topics that are covered in typical "discrete math"/"math for CS" courses currently offered in most CS departments.
- *Advanced undergraduate/beginning graduate introduction to complexity course.* The book can be used as a text for an introductory complexity course aimed at undergraduate or non-theory graduate students (replacing Papadimitriou's 1994 book [Pap94] that does not contain many recent results). Such a course would probably include many topics from Part I and then a sprinkling from Parts II and III, and assume some background in algorithms and/or the theory of computation.
- *Graduate Complexity course.* The book can serve as a text for a graduate complexity course that prepares graduate students interested in theory to do research in complexity and related areas. Such a course can use parts of Part I to review basic material, and then move on to the advanced topics of Parts II and III. The book contains far more material than can be taught in one term, and we provide on our website several alternative outlines for such a course.

We hope that this book conveys our excitement about this new field and the insights it provides in a host of older disciplines.

Contents