Preface

This book is a slight revision of my doctoral dissertation, which was completed in December 1988 at the University of California at Berkeley under the supervision of Richard Karp. The subject of this thesis is pseudorandom generators, functions that stretch a short random string to a long string that "looks" random. This notion was introduced in the early 1980's by M. Blum, S. Micali, and A. Yao, who also observed that the construction of such pseudorandom generators is dependent upon the computational hardness of certain problems. Here we continue exploring the connection between computational hardness and pseudorandom generation and present two different constructions of pseudorandom generators, which are based upon the hardness of certain problems.

Our first construction is simple and very general. We construct pseudorandom generators that produce strings that look random to any algorithm from a complexity class C (e.g. P, NC, $PSPACE$, etc.) using an *arbitrary* function that is hard for C. This construction reveals an *equivalence* between the problems of proving certain lower bounds and of constructing pseudorandom generators.

This construction has many consequences. The most direct one is that efficient deterministic simulation of randomized algorithms is possible under much weaker assumptions than previously known. The efficiency of the simulations depends on the strength of the assumptions and may achieve $P = BPP$. We believe that our results are very strong evidence that the gap between randomized and deterministic complexity is not large.

Using the known lower bounds for constant depth circuits, our construction yields unconditionally proven pseudorandom generators for constant depth circuits. As an application we characterize the power of NP with a random oracle.

Our second pseudorandom generator produces strings that look random to all *Logspace* machines. This is proved without relying on any unproven assumptions. Instead, we use lower bounds on the complexity of the following multiparty communication game:

Let $f(x_1, ..., x_k)$ be a Boolean function that k parties wish to collaboratively evaluate. The i'th party knows each input argument except x_i, and each party has unlimited computational power. They share a blackboard, viewed by all parties, where they can exchange messages. The objective is to minimize the number of bits written on the board.

We prove lower bounds on the number of bits that need to be written on the board in order to compute a certain function. We then use these bounds to construct a pseudorandom generator for Logspace. As an application we present an explicit construction of universal traversal sequences for general graphs.