Statistical Science
1993, Vol. 8, No. 1, 1–2

In This Issue

This issue of *Statistical Science* is devoted to a report on probability and algorithms prepared under the supervision of a panel selected by the Committee on Applied and Theoretical Statistics of the National Research Council. In organizational structure, the Committee on Applied and Theoretical Statistics is part of the Board on Mathematical Sciences, which in turn is part of the Commission on Physical Sciences, Mathematics and Applications of the National Research Council. The National Research Council is the principal operating agency of the National Academy of Sciences.

The articles reprinted here view the interface of probability and algorithms from an uncommonly wide range of perspectives. Some of the articles recall the evolving confluence between the traditional concerns of the theory of algorithms and technology of applied probability; but others reveal how theoretical computer scientists have spawned new varieties of computational complexity to deal with the use of randomized methods, how probability can guide the development of methods that preserve privacy or how issues of hardware design are now informed by probabilistic insights.

The article "Simulated Annealing" by Bertsimas and Tsitsiklis offers a natural start by giving a succinct reprise of a famous method that calls on the theory of Markov chains to provide a strategy for maximizing a function defined on a finite set. One of the great charms of simulated annealing is its extraordinary generality. Almost any optimization problem can be approached by simulated annealing, and often the coding is quite easy. Still, considerable analytical finesse is required for a deep understanding of the behavior of simulated annealing, and, even after several years of intense investigation of the method, there remain basic questions, not the least of which concern the validity of the statistical mechanics metaphor that first set the ball rolling.

The next article, "Approximate Counting via Markov Chains," by Aldous recalls another basic means by which Markov chains have found powerful uses in combinatorial calculations. The key observation is that there is an intimate relationship between having an explicit formula for the cardinality of a finite set S and having a fast algorithm for choosing an element of S at random according to the uniform distribution. This relationship has been exploited to provide new algorithms for determining the volume of a convex set in $\mathbb{R}^d$, for computing the number of matchings in a graph and for many other problems. This line of investigation is part of a renaissance that is underway in the theory of Markov chains. The fundamental question often comes down to knowing how long a Markov chain must run before reaching approximate stationarity. This question may seem classic, but its life has been transformed by a world of new applications and powerful new tools, like Cheeger's inequality, which has been imported from the field of differential geometry.

The next article, "Probabilistic Algorithms for Speedup," by Feigenbaum and Lagarias begins with a basic introduction to the probabilistic complexity classes that have become of great importance in theoretical computer science. It follows through with practical illustrations of probabilistic speedups in prime testing and integer factorization. In the final section, it develops the connection between probabilistic speedup and communication complexity, a fascinating new topic initiated by Andrew Yao that asks how many messages two people must exchange to compute $f(x, y)$ if one of them knows x and the other knows y.

Of all the notions of theoretical computer science that have been developed in the last dozen years, those that speak to the preservation of privacy seem to exert a particular fascination. In her article "Probabilistic Algorithms for Defeating Adversaries," Feigenbaum introduces us to the role of probability in addressing the private use of shared resources. Important connections subsequently are made to the notions of zero-knowledge proof systems and of *authentication*, a topic that has numerous applications—even down to our everyday experience with automated teller machines.

In the last of the suite of articles focusing on probability and computational complexity is "Pseudorandom Numbers" by Lagarias. Statisticians and probabilists familiar with the classic uses of pseudorandom numbers will find that theoretical computer scientists put a very different set of issues in play. One of the most fascinating of these is the connection between computational complexity and one-way functions.

Statisticians and probabilists may feel that they have returned to more familiar ground on turning to the essay "Probabilistic Analysis of Packing and Related Partitioning Problems" by Coffman, Johnson, Lueker and Shor. Some of the issues the authors engage can be well understood on the factory floor, since, after all, that is where they originated. Still, the analyses evolving in the area they survey offer layers of depth that will call for years of further exploration.

In the article "Probability and Problems in Euclidean Combinatorial Optimization," the focus is on problems like the traveling salesman problem, minimal spanning tree and minimal matching that have long been at the center of algorithmic investigations, and evidence is rapidly accumulating that they also offer vital challenges to probabilists.

When one speaks of algorithms and paradigms that