81st Josiah Willard Gibbs Lecture
Sunday, January 6, 2008
8:30 p.m.

JOSIAH WILLARD GIBBS 1839–1903

Photograph by Pictorial Mathematics
Scripta Mathematica
Yeshiva College, New York, 1942
Josiah Willard Gibbs Lecture

Sunday, January 6, 2008
8:30 p.m.

Room 6 AB
San Diego Convention Center
San Diego, California

Randomness—A Computational Complexity View

Avi Wigderson
Institute for Advanced Study
Princeton, New Jersey

To commemorate the name of Professor Gibbs, the American Mathematical Society established an honorary lectureship in 1923 to be known as the Josiah Willard Gibbs Lectureship. The lectures are of a semipopular nature and are given by invitation. They are usually devoted to mathematics or its applications. It is hoped that these lectures will enable the public and the academic community to become aware of the contribution that mathematics is making to present-day thinking and to modern civilization.
Abstract

Man has grappled with the meaning and utility of randomness for centuries. Research in the Theory of Computation in the last thirty years has enriched this study considerably. I’ll describe two main aspects of this research on randomness, demonstrating its power and weakness respectively.

–Randomness is paramount to computational efficiency:

The use of randomness can dramatically enhance computation (and do other wonders) for a variety of problems and settings. In particular, examples will be given of probabilistic algorithms (with tiny error) for natural tasks in different areas of mathematics, which are exponentially faster than their (best known) deterministic counterparts.

–Computational efficiency is paramount to understanding randomness:

I will explain the computationally-motivated definition of pseudo-random distributions, namely ones which cannot be distinguished from the uniform distribution by efficient procedure from a given class. We then show how such pseudorandomness may be generated deterministically, from (appropriate) computationally difficult problems. Consequently, randomness is probably not as powerful as it seems above.

I’ll conclude with the power of randomness in other computational settings, primarily probabilistic proof systems. We discuss the remarkable properties of Zero-Knowledge proofs and of Probabilistically Checkable proofs.
Avi Wigderson

Avi Wigderson is a Professor at the School of Mathematics, Institute for Advanced Study. He obtained his B.Sc. in Computer Science from the Technion in 1980, and his Ph.D. from Princeton in 1983. He was a member of the faculty at the Hebrew University in Jerusalem from 1986–2003, and is currently a member of the Mathematics Faculty at the Institute for Advanced Study at Princeton. He joined the permanent faculty of the Institute for Advanced Study in 1999. His research interests lie principally in Complexity Theory, Algorithms, Randomness, and Cryptography. His awards include the Nevanlinna Prize (1994).
Gibbs Lectures

1. February 1924, New York City; Professor Michael I. Pupin, Columbia University; Coordination, Scribner’s Magazine, v. 76, no. 1, pp. 3–10 (1925).
7. December 1929, Des Moines, Iowa; Professor Irving Fisher, Yale University; The applications of mathematics to the social sciences, Bulletin of the American Mathematical Society, v. 36, no. 4, pp. 225–243 (1930).
11. December 1934, Pittsburgh, Pennsylvania; Professor Albert Einstein, Institute for Advanced Study; An elementary proof of the theorem concerning the equivalence of mass and energy, Bulletin of the American Mathematical Society, v. 41, no. 4, pp. 225–230 (1935).
15. December 1939, Columbus, Ohio; Professor Theodore von Kármán, California Institute of Technology; The engineer grapples with nonlinear problems, Bulletin of the American Mathematical Society, v. 46, no. 8, pp. 615–683 (1940).
November 1944, Chicago, Illinois; Professor John von Neumann, Institute for Advanced Study; *The ergodic theorem and statistical mechanics*.


December 1947, Athens, Georgia; Professor P. M. Morse, Massachusetts Institute of Technology; *Mathematical problems in operations research*, Bulletin of the American Mathematical Society, v. 54, no. 7, pp. 602–621 (1948).

December 1948, Columbus, Ohio; Professor Hermann Weyl, Institute for Advanced Study; *Ramifications, old and new, of the eigenvalue problem*, Bulletin of the American Mathematical Society, v. 56, no. 2, pp. 115–139 (1950).


December 1950, Gainesville, Florida; Professor G. E. Uhlenbeck, University of Michigan; *Some basic problems of statistical mechanics*.

December 1951, Providence, Rhode Island; Professor Kurt Gödel, Institute for Advanced Study; *Some basic theorems on the foundations of mathematics and their philosophical implications*. First published in his *Collected Works*, v. III, Oxford University Press, pp. 304–323 (1995). Published title omits the word “philosophical”.

December 1952, St. Louis, Missouri; Professor Marston Morse, Institute for Advanced Study; *Topology and geometrical analysis*.


January 1958, Cincinnati, Ohio; Professor H. J. Muller, Department of Zoology, Indiana University; *Evolution by mutation*, Bulletin of the American Mathematical Society, v. 64, no. 4, pp. 137–160 (1958).


January 1960, Chicago, Illinois; Professor Julian Schwinger, Harvard University; *Quantum field theory*.


January 1962, Cincinnati, Ohio; Professor C. N. Yang, Institute for Advanced Study; *Symmetry principles in modern physics*.

January 1963, Berkeley, California; Professor Claude E. Shannon, Massachusetts Institute of Technology; *Information theory*.

January 1964, Miami, Florida; Professor Lars Onsager, Yale University; *Mathematical problems of cooperative phenomena*.


40. January 1967, Houston, Texas; Professor Mark Kac, Rockefeller University; *Some mathematical problems in the theory of phase transitions*.


46. January 1973, Dallas, Texas; Professor Jürgen Moser, Courant Institute of Mathematical Sciences, New York University; *The stability concept in dynamical systems*.

47. January 1974, San Francisco, California; Professor Paul A. Samuelson, Massachusetts Institute of Technology; *Economics and mathematical analysis*.


49. January 1976, San Antonio, Texas; Professor Arthur S. Wightman, Princeton University; *Nonlinear functional analysis and some of its applications in quantum field theory*.


52. January 1979, Biloxi, Mississippi; Professor Martin Kruskal, Princeton University; “What are solitons and inverse scattering anyway, and why should I care?”

53. January 1980, San Antonio, Texas; Professor Kenneth Wilson, Cornell University; *The statistical continuum limit*.


6

58. January 1985, Anaheim, California; Professor Michael O. Rabin, Harvard University, Cambridge, Massachusetts and Hebrew University, Jerusalem, Israel; Randomization in mathematics and computer science.

59. January 1986, New Orleans, Louisiana; Professor L. E. Scriven, University of Minnesota; The third leg: Mathematics and computation in applicable science and high technology.

60. January 1987, San Antonio, Texas; Professor Thomas C. Spencer, Courant Institute of Mathematical Sciences, New York University; Schrödinger operators and dynamical systems.


63. January 1990, Louisville, Kentucky; Professor George B. Dantzig, Stanford University, Stanford, California; The wide wide world of pure mathematics that goes by other names.


65. January 1992, Baltimore, Maryland; Professor Michael E. Fisher, Institute for Physical Sciences and Technology, University of Maryland, College Park, Maryland; Approaching the limit: Mathematics and myth in statistical physics.

66. January 1993, San Antonio, Texas; Professor Charles S. Peskin, Courant Institute of Mathematical Sciences, New York University; Fluid dynamics and fiber architecture of the heart and its valves.


68. January 1995, San Francisco, California; Professor Andrew J. Majda, Princeton University; Turbulence, turbulent diffusion, and modern applied mathematics.

69. January 1996, Orlando, Florida; Professor Steven Weinberg, University of Texas, Austin; Is field theory the answer? Is string theory the answer? What was the question?


72. January 1999, San Antonio, Texas; Professor Nancy J. Kopell, Boston University; We got rhythm; Dynamical systems of the nervous system, Notices of the American Mathematical Society, v. 47 no. 1, pp. 6–16 (2000).

73. January 2000, Washington, DC; Professor Roger Penrose, Mathematical Institute, Oxford University; Physics, computability, and mentality.

74. January 2001, New Orleans, Louisiana; Professor Ronald L. Graham, University of California, San Diego; The Steiner problem.


76. January 2003, Baltimore, Maryland; Professor David B. Mumford, Division of Applied Mathematics, Brown University, Providence, RI; The shape of objects in two and three dimensions: Mathematics meets computer vision.
77. January 2004, Phoenix, Arizona; Professor Eric S. Lander, Professor of Biology, Massachusetts Institute of Technology, Cambridge, Massachusetts; Biology as information.

78. January 2005, Atlanta, Georgia; Professor Ingrid Daubechies, Department of Mathematics and Program in Applied and Computational Mathematics, Princeton University, Princeton, New Jersey; The interplay between analysis and algorithms.

79. January 2006, San Antonio, Texas; Professor Michael A. Savageau, Department of Biomedical Engineering and Microbiology Graduate Group, University of California, Davis, California; Function, design, and evolution of gene circuitry.

80. January 2007, New Orleans, Louisiana; Professor Peter D. Lax, Courant Institute of Mathematical Sciences, New York University, New York, New York; Mathematics and physics.

81. January 2008, San Diego, California; Professor Avi Wigderson, Institute for Advanced Study, Princeton, New Jersey; Randomness—A computational complexity view.