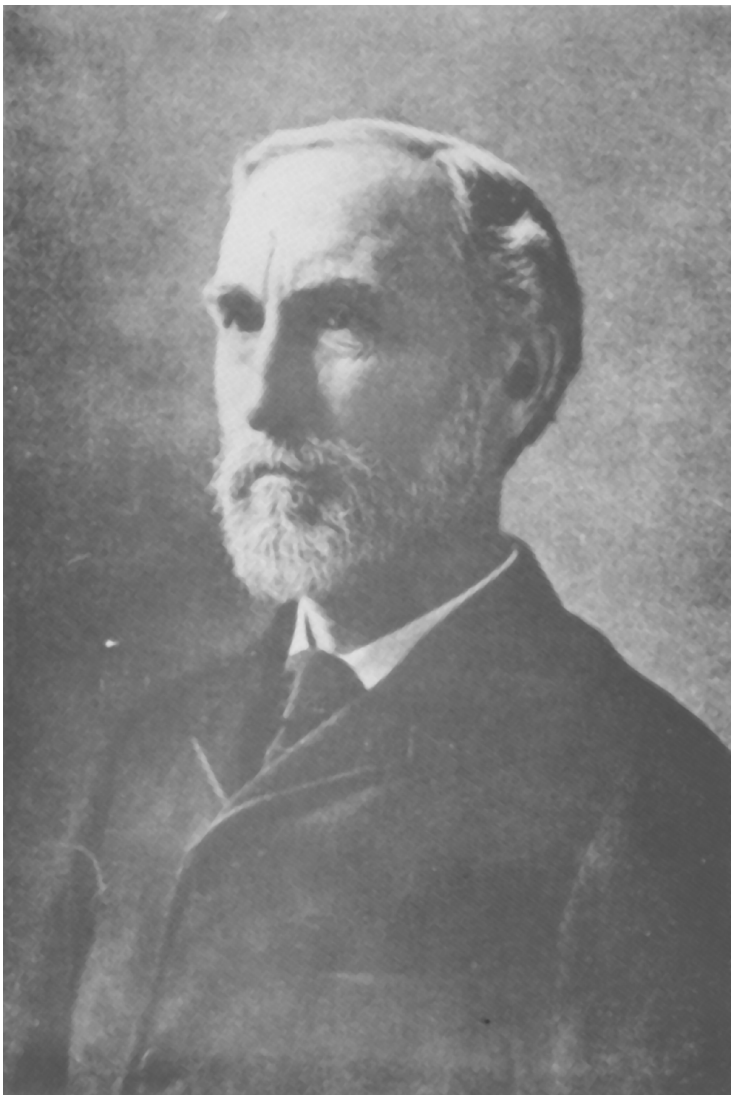
81st Josiah Willard Gibbs Lecture

Sunday, January 6, 2008

8:30 p.m.



JOSIAH WILLARD GIBBS 1839–1903

Photograph by Pictorial Mathematics
Scripta Mathematica
Yeshiva College, New York, 1942

American Mathematical Society

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).
2. December 1924, Washington, D.C.; Dr. Robert Henderson, Vice President, Equitable Life Assurance Society of the U.S.; *Life insurance as a social science and as a mathematical problem*, Bulletin of the American Mathematical Society, v. 31, nos. 5–6, pp. 227–252 (1925).
3. December 1925, Kansas City, Missouri; Professor James Pierpont, Yale University; *Some modern views of space*, Bulletin of the American Mathematical Society, v. 32, no. 3, pp. 225–258 (1926).
4. December 1926, Philadelphia, Pennsylvania; Professor H. B. Williams, Columbia University; *Mathematics and the biological sciences*, Bulletin of the American Mathematical Society, v. 33, no. 3, pp. 273–293 (1927).
5. December 1927, Nashville, Tennessee; Professor E. W. Brown, Yale University; *Resonance in the solar system*, Bulletin of the American Mathematical Society, v. 34, no. 3, pp. 265–289 (1928).
6. December 1928, New York City; Professor G. H. Hardy, Trinity College (England); *An introduction to the theory of numbers*, Bulletin of the American Mathematical Society, v. 35, no. 6, pp. 778–818 (1929).
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).
8. December 1930, Cleveland, Ohio; Professor E. B. Wilson, Harvard School of Public Health; *Reminiscences of Gibbs by a student and colleague*, Bulletin of the American Mathematical Society, v. 37, no. 6, pp. 401–416 (1931).
9. December 1931, New Orleans, Louisiana; Professor P. W. Bridgman, Harvard University; *Statistical mechanics and the second law of thermodynamics*, Bulletin of the American Mathematical Society, v. 38, no. 4, pp. 225–245 (1932).
10. December 1932, Atlantic City, New Jersey; Professor R. C. Tolman, California Institute of Technology; *Thermodynamics and relativity*, Bulletin of the American Mathematical Society, v. 39, no. 2, pp. 49–74 (1933).
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. 223–230 (1935).
12. January 1935, St. Louis, Missouri; Dr. Vannevar Bush, Vice President, Massachusetts Institute of Technology; *Mechanical analysis*, Bulletin of the American Mathematical Society, v. 42, no. 10, pp. 649–670 (1936).
13. October 1936, New York City; Professor H. N. Russell, Princeton University; *Model stars*, Bulletin of the American Mathematical Society, v. 43, no. 2, pp. 49–77 (1937).
14. December 1937, Indianapolis, Indiana; Professor C. A. Kraus, Brown University; *The present status of the theory of electrolytes*, Bulletin of the American Mathematical Society, v. 44, no. 6, pp. 361–383 (1938).
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).
16. September 1941, Chicago, Illinois; Professor Sewall Wright, University of Chicago; *Statistical genetics and evolution*, Bulletin of the American Mathematical Society, v. 48, no. 4, pp. 223–246 (1942).
17. November 1943, Chicago, Illinois; Professor Harry Bateman, California Institute of Technology; *The control of elastic fluids*, Bulletin of the American Mathematical Society, v. 51, no. 9, pp. 601–646 (1945).

18. November 1944, Chicago, Illinois; Professor John von Neumann, Institute for Advanced Study; *The ergodic theorem and statistical mechanics*.
19. November 1945, Chicago, Illinois; Professor J. C. Slater, Massachusetts Institute of Technology; *Physics and the wave equation*, Bulletin of the American Mathematical Society, v. 52, no. 5, part 1, pp. 392–400 (1946).
20. November 1946, Swarthmore, Pennsylvania; Professor Subrahmanyan Chandrasekhar, University of Chicago; *The transfer of radiation in stellar atmosphere*, Bulletin of the American Mathematical Society, v. 53, no. 7, pp. 641–711 (1947).
21. 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).
22. 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).
23. December 1949, New York City; Professor Norbert Wiener, Massachusetts Institute of Technology; *Problems of sensory prosthesis*, Bulletin of the American Mathematical Society, v. 57, no. 1, pp. 27–35 (1951).
24. December 1950, Gainesville, Florida; Professor G. E. Uhlenbeck, University of Michigan; *Some basic problems of statistical mechanics*.
25. 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".
26. December 1952, St. Louis, Missouri; Professor Marston Morse, Institute for Advanced Study; *Topology and geometrical analysis*.
27. December 1953, Baltimore, Maryland; Professor Wassily Leontief, Harvard University; *Mathematics in economics*, Bulletin of the American Mathematical Society, v. 60, no. 3, pp. 215–233 (1954).
28. December 1954, Pittsburgh, Pennsylvania; Professor Kurt O. Friedrichs, Institute of Mathematical Sciences, New York University; *Asymptotic phenomena in mathematical physics*, Bulletin of the American Mathematical Society, v. 61, no. 6, pp. 485–504 (1955).
29. December 1955, Houston, Texas; Professor Joseph E. Meyer, University of Chicago; *The structure of simple fields*, Bulletin of the American Mathematical Society, v. 62, no. 4, pp. 332–346 (1956).
30. December 1956, Rochester, New York; Professor Marshall H. Stone, University of Chicago; *Mathematics and the future of science*, Bulletin of the American Mathematical Society, v. 63, no. 2, pp. 61–76 (1957).
31. 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).
32. January 1959, Philadelphia, Pennsylvania; Professor J. M. Burgers, University of Maryland; *On the emergence of patterns of order*, Bulletin of the American Mathematical Society, v. 69, no. 1, pp. 1–25 (1963).
33. January 1960, Chicago, Illinois; Professor Julian Schwinger, Harvard University; *Quantum field theory*.
34. January 1961, Washington, D.C.; Professor J. J. Stoker, Institute of Mathematical Sciences, New York University; *Some nonlinear problems in elasticity*, Bulletin of the American Mathematical Society, v. 68, no. 4, pp. 239–278 (1962). Published under the title *Some observations on continuum mechanics with emphasis on elasticity*.
35. January 1962, Cincinnati, Ohio; Professor C. N. Yang, Institute for Advanced Study; *Symmetry principles in modern physics*.
36. January 1963, Berkeley, California; Professor Claude E. Shannon, Massachusetts Institute of Technology; *Information theory*.
37. January 1964, Miami, Florida; Professor Lars Onsager, Yale University; *Mathematical problems of cooperative phenomena*.

38. January 1965, Denver, Colorado; Professor D. H. Lehmer, University of California, Berkeley; *Mechanical mathematics*, Bulletin of the American Mathematical Society, v. 72, no. 5, pp. 739–750 (1966).
39. January 1966, Chicago, Illinois; Professor Martin Schwarzschild, Princeton University; *Stellar evolution*.
40. January 1967, Houston, Texas; Professor Mark Kac, Rockefeller University; *Some mathematical problems in the theory of phase transitions*.
41. January 1968, San Francisco, California; Professor Eugene P. Wigner, Princeton University; *Problems of symmetry in old and new physics*, Bulletin of the American Mathematical Society, v. 74, no. 5, pp. 793–815 (1968).
42. January 1969, New Orleans, Louisiana; Professor Raymond L. Wilder, University of Michigan; *Trends and social implications of research*, Bulletin of the American Mathematical Society, v. 75, no. 5, pp. 891–906 (1969).
43. January 1970, San Antonio, Texas; Professor Walter H. Munk, Institute of Geophysics and Planetary Physics and the Scripps Institution of Oceanography, University of California, San Diego; *Tides and time*.
44. January 1971, Atlantic City, New Jersey; Professor Eberhard F. F. Hopf, Indiana University; *Ergodic theory and the geodesic flow on surfaces of constant negative curvature*, Bulletin of the American Mathematical Society, v. 77, no. 6, pp. 863–877 (1971).
45. January 1972, Las Vegas, Nevada; Professor Freeman J. Dyson, Institute for Advanced Study; *Missed opportunities*, Bulletin of the American Mathematical Society, v. 78, no. 5, pp. 635–652 (1972).
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*.
48. January 1975, Washington, D.C.; Professor Fritz John, Courant Institute of Mathematical Sciences, New York University; *A priori estimates, geometric effects, and asymptotic behavior*, Bulletin of the American Mathematical Society, v. 81, no. 6, pp. 1013–1023 (1975).
49. January 1976, San Antonio, Texas; Professor Arthur S. Wightman, Princeton University; *Nonlinear functional analysis and some of its applications in quantum field theory*.
50. January 1977, St. Louis, Missouri; Professor Joseph B. Keller, Courant Institute of Mathematical Sciences, New York University; *Rays, waves, and asymptotics*, Bulletin of the American Mathematical Society, v. 84, no. 5, pp. 727–750 (1978).
51. January 1978, Atlanta, Georgia; Professor Donald E. Knuth, Stanford University; *Mathematical typography*, Bulletin of the American Mathematical Society (N.S.), v. 1, no. 2, pp. 337–372 (1979).
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*.
54. January 1981, San Francisco, California; Professor Cathleen S. Morawetz, Courant Institute of Mathematical Sciences, New York University; *The mathematical approach to the sound barrier*, Bulletin of the American Mathematical Society (N.S.), v. 6, no. 2, pp. 127–145 (1982). Published under the title *The mathematical approach to the sonic barrier*.
55. January 1982, Cincinnati, Ohio; Professor Elliott W. Montroll, Institute for Physical Science and Technology, University of Maryland, College Park, Maryland; *The dynamics and evolution of some sociotechnical systems*, Bulletin of the American Mathematical Society (N.S.), v. 16, no. 1, pp. 1–46 (1987).
56. January 1983, Denver, Colorado; Professor Samuel Karlin, Stanford University, Stanford, California; *Mathematical models and controversies of evolutionary theory*, Bulletin of the American Mathematical Society (N.S.), v. 10, no. 2, pp. 221–273 (1984). Published under the title *Mathematical models, problems, and controversies of evolutionary theory*.

57. January 1984, Louisville, Kentucky; Professor Herbert A. Simon, Carnegie-Mellon University, Pittsburgh, Pennsylvania; *Computer modeling of the processes of scientific and mathematical discovery*, Bulletin of the American Mathematical Society (N.S.), v. 11, no. 2, pp. 247–262 (1984). Published under the title *Computer modeling of scientific and mathematical discovery processes*.
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*.
61. January 1988, Atlanta, Georgia; Professor David P. Ruelle, Institut des Hautes Études Scientifiques, Paris, France; *How natural is our mathematics? The example of equilibrium statistical mechanics*, Bulletin of the American Mathematical Society (N.S.), v. 19, no. 2, pp. 259–268 (1988). Published under the title *Is our mathematics natural? The case of equilibrium statistical mechanics*.
62. January 1989, Phoenix, Arizona; Professor Elliott H. Lieb, Princeton University, Princeton, New Jersey; *The stability of matter*: *from atoms to stars*, Bulletin of the American Mathematical Society (N.S.), v. 22, no. 1, pp. 1–49 (1990).
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*.
64. January 1991, San Francisco, California; Sir Michael Atiyah, FRS, Trinity College, Cambridge, England; *Physics and the mysteries of space*; Selected Lectures, AMS videotape.
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*.
67. January 1994, Cincinnati, Ohio; Professor Robert M. May, Oxford University; *Necessity and chance*: *Deterministic chaos in ecology and evolution*, Bulletin of the American Mathematical Society (N.S.), v. 32, no. 3, pp. 291–308 (1995) .
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?*
70. January 1997, San Diego, California; Professor Persi Diaconis, Department of Mathematics, Harvard University; *Patterns in eigenvalues*, Bulletin of the American Mathematical Society (N.S.), v. 40, no. 2, pp. 155–178 (2003).
71. January 1998, Baltimore, Maryland; Professor Edward Witten, School of Natural Sciences, Institute for Advanced Study; *M-Theory*, Notices of the American Mathematical Society, v. 45, no. 9, pp. 1124–1129 (1999). Published under the title *Magic, mystery, and matrix*.
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*.
75. January 2002, San Diego, California; Professor Michael V. Berry, Physics Department, Bristol University, UK; *Making light of mathematics*, Bulletin of the American Mathematical Society (N.S.), v. 40, no. 2, pp. 229–237 (2003).
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*.