MANUEL BLUM

Bruce Nelson Professor of Computer Science
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213

Telephone: Office: (412) 268-3742, Fax: (412) 268-5576
Home: (412) 687-8730, Mobile: (412) 596-4063
Email: mblum@cs.cmu.edu

Personal

Born: 26 April1938 in Caracas, Venezuela.
Citizenship: Venezuela and USA.
Naturalized Citizen of USA, January 2000.

Wife: Lenore Blum, Distinguished Career Professor of Computer Science, CMU
Son: Avrim Blum, Professor of Computer Science, CMU.

Interests: Computational Complexity; Automata Theory; Algorithms; Inductive Inference: Cryptography; Program Result-Checking; Human Interactive Proofs.

Employment History

Research Assistant and Research Associate for Dr. Warren S. McCulloch, Research Laboratory of Electronics, MIT, 1960-1965.

Assistant Professor, Department of Mathematics, MIT, 1966-68.

Visiting Assistant Professor, Associate Professor, Professor, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, 1968-2001.

Associate Chair for Computer Science, U.C. Berkeley, 1977-1980.
Arthur J. Chick Professor of Computer Science, U.C. Berkeley, 1995-2001.

Group in Logic and Methodology of Science, U.C. Berkeley, 1974-present.

Visiting Professor of Computer Science. City University of Hong Kong, 1997-1999.

Bruce Nelson Professor of Computer Science, Carnegie Mellon University, 2001-present.

Education

B.S., Electrical Engineering, MIT, 1959; M.S., Electrical Engineering, MIT. 1961.
Ph.D., Mathematics, MIT, 1964, Professor Marvin Minsky, supervisor.

Honors

MIT Class VIB (Honor Sequence in EE), 1958-61

Sloan Foundation Fellowship, 1972-73.

U.C. Berkeley Distinguished Teaching Award, 1977.

Fellow of the IEEE "for fundamental contributions to the abstract theory of computational complexity," 1982.

Fellow of the American Association for the Advancement of Science, 1983.

Sigma Xi's Monie A. Ferst award for "notable contributions to motivation and encouragement of research through education," 1991.

Faculty Research Lechtrer, Berkeley, 1995.

Fellow of the *American Academy of Arts and Sciences*, 1995.

ACM's 1995 *Alan M. Turing* award for "contributions to the foundations of computational complexity theory and its application to cryptography and program checking."

U.S. *National Academy of Science*, 2002.

Herbert A. Simon Teaching Award*,* 8 May 2007

Publications

1. "Properties of a Neuron with Many Inputs," Bionics Symposium, *WADD Technical Report 60-600* (September 1960), 55-82.

2. "Machine-Dependence of Degrees of Difficulty," (with M. Arbib), *Proceedings of the AMS*, XVI, No. 3 (June 1965), 442-447.

3. "Recursive Function Theory and Speed of Computation," *Can. Math. Bull.,* IX, No. 6 (1966), 745-750.

4. "A Machine-Independent Theory of the Complexity of Recursive Functions," *JACM,* XIV, No. 2 (Apri11967), 322-336.

5. "On the Size of Machines," *Information and Control,* XI, No.3 (September 1967), 257-265.

6. "Automata on a 2-dimensional Tape," (with C. Hewitt), *IEEE Conference Record: Eighth Annual Symposium on Switching and Automata Theory* (October 1967), 155-160.

7. "Any Two Universal Partial Functions are Recursively Isomorphic," in H.J. Rogers, Jr. *Theory of Recursive Functions and Effective Computability,* McGraw-Hill (1967), 191.

8. "Tape Reversal Complexity Hierarchies." (with P .C. Fisher and J. Hartmanis), in *Conf Record, 1968 Ninth Annual Symposium on Switching and Automata Theory,* New York (October 1968), 373-382.

9. "On Effective Procedures for Speeding Up Algorithms," *Proc. ACM Symposium on Theory of Computing (May 1969), 43-54, and Journal Association for Computing Machinery,* Vol. 18. No.2 (April1971), 290-305.

10. "Some Fruitful Areas for Research into Complexity Theory," (with J. Gill), in *Computational Complexity. Courant Computer Science Symposium 7,* ed. Randall Rustin, Algorithmics Press (October 1971), 23-36.

11. "Linear Time Bounds for Median Computations," (with Floyd, Pratt, Rivest, and Tarjan), *Proc.4th Annual ACM Symposium on Theory of Computing,* Denver, Colorado (May 1972), 119-124.

12. "Inductive Inference: a Recursion Theoretic Approach," (with L. Blum), *Annual Symposium on Switching and Automata Theory* (October 15-17, 1973), 200-208.

13. "On Complexity Properties of Recursively Enumerable Sets," (with I. Marques), *Journal of Symbolic Logic,* Vol. 38, No.4 (December 1973), 579-593.

14. "On Almost Everywhere Complex Recursive Ftmctions," (with J. Gill), *Journal ACM,* Vol. 21, No.3 (July 1974), 425-435.

15. "Toward a Mathematical Theory of Inductive Inference," (with L. Blum), *Information and Control,* Vol. 28 (June 1975), 125-155.

16. "On the Capability of Finite Automata in 2 and 3 Dimensional Space," (with W. Sakoda), *Proc. 18th IEEE FOCS Conf* (1977), 147-161.

17. "On the Power of the Compass (or, Why Mazes are Easier to Search Than Graphs)," (with D. Kozen), *Proc. 19th IEEE FOCS Conf* (1978), 132-142.

18. "Equivalence of Free Boolean Graphs Can Be Decided Probabilistically in Polynomial Time," (with A.K. Chandra and M.N. Wegman), *Information Processing Letters,* Vol. 10, No.2 (March 1980), 80-82.

19. "Inductive Inference and Unsolvability," (with L. Adleman), *The Journal of Symbolic Logic,* Vol. 56, No.3, 891-900, September 1991.

20. "The Complexity of Testing Whether a Graph Is a Superconcentrator," (with R.M. Karp, C.H. Papadimitriou, 0. Vornberger, and M. Yannakakis), *Information Processing Letters,* Vol. 13, Nos. 4, 5 (Nov-Dec. 1981), 164-167.

21. "Coin Flipping by Telephone: A Protocol for Solving Impossible Problems," *Proc. Compcon 82 Conference, San Francisco* (Feb 1982), 133-137. (CRYPTO 1981: 11-15)

22. "How to Exchange (Secret) Keys," *ACM Transactions on Computing Systems* (by invitation), Vol. 1, No.2 (May 1983), 175-193.

23. "How to Send Certified Electronic Mail," (with M.O. Rabin)

24. "How to Generate Cryptographically Strong Sequences of Pseudo Random Bits," (with S. Micali), *SIAM f. Computing* Vol. 13, No.4 (Nov 1984), 850-864.

25. "A Simple Unpredictable Pseudo-Random Number Generator," (with L. Blum and M. Shub), *SIAM J. Computing,* Vol. 15, No.2 (May 1986), 364-382.

26. "Independent Unbiased Coin Flips From a Correlated Biased Source, a Finite State Markov Chain," *Proc. 25th IEEE FOCS* (Oct 1984) ,425-433, and (by invitation to special FOCS issue) *Combinatorica,* Vol. 6, No.2 (1986), 97-108.

27. "How to Prove a Theorem So No One Else Can Claim It," Invited 45-minute address to the International Congress of Mathematicians, 1986; *Proceedings of the 1986 International Congress of Mathematicians. American Mathematical Society,* 1987, 1444-1451.

28. "Generic Oracles and Oracle Classes" (with Russell Impagliazzo), *28th IEEE Symposium on Foundations of Computer Science* (FOCS), Oct 1987, 118-126.

29. "Non-Interactive Zero-Knowledge and Its Applications" (with P. Feldman and S. Micah), *20th ACM Symposium on Theory of Computing* (STOC), May 1988, 103-112.

30. "Reversing Trains: A Tum of the Century Sorting Problem" (with N. Amato, S. Irani, and R. Rubinfeld), *J. of Algorithms,* Vol. 10 (1989), 413-428. M. Blum and P. Raghavan.

31. "Program Correctness: Can One Test for It?" invited/ appeared in *IFIP 89,* edited by G. X. Ritter, Elsevier Science Publications B.V. (North-Holland), (September 1989), pp. 127-134.

32. "Designing Programs to Check Their Work," *ICSI Technical Report TR-88-009* (November 1988), 21 pp.

33. "Designing Programs That Check Their Work" (with S. Kannan), in *Proc. of the 21'1 Annual ACM Symposium on Theory of Computing* (May 1989), pp. 86-97; and in *JACM* (with M. Luby, and R. Rubinfeld), Vol. 42, No.1, 269-291, 1995.

34. "Self-Testing/Correcting with Applications to Numerical Problems" (with P. Feldman, and S. Micali), *STOC 90* (May 1990), 10 pp.

35. "Proving Security Against Chosen Ciphertext Attacks" (with A. de Santis, S. Micali, and G. Persiano), in *Advances in Cryptology- CRYPTO '88,* ed. S. Goldwasser, in the Springer-Verlag Series Lecture Notes in Computer Science (1990), 256-268.

36. "Noninteractive Zero-Knowledge" (with M. Luby, and R. Rubinfe1d), *SlAM J. Comput,* Vol. 20, No.6, (1991), 1084-1118.

37. "Program Result Checking against Adaptive Programs and in Cryptographic Settings" in *Distributed Computing and Cryptography,* ed. J. Feigenbaum and M. Merritt, AMS and ACM publishers, (1991), 107-118.

38. "Checking the Correctness of Memories" (with W. Evans, P. Gemmell, and S. Kannan); *FOCS 91* (Oct 91), 90-99.

39. "Program Checking," in *Foundations of Software Technology and Theoretical Computer Science. Proc. of 11th conference, New Delhi, India,* ed. S. Biswas and K.V. Nori, Springer-Verlag Lecture Notes in Computer Science 560 (Dec 1991), 1-9.

40. "Universal Statistical Tests" (with 0. Goldreich), in *LATIN'92 -1st Latin American Symposium on Theoretical Informatics,* ed. I. Simon, Springer-Verlag Lecture Notes in Computer Science 583. (April1992), 71-75.

41. "Towards a Computational Theory of Statistical Tests." (with S. Ar, B. Codenotti, and P. Gemmell), *33rd Annual IEEE Symposium on Foundations of Computer Science (FOCS),* Pittsburgh PA, 406-416, October 24-27,1992.

42. "Checking approximate Computations over the Reals," *25th Annual ACM Symposium on the Theory of Computing (STOC),* San Diego CA, 786-795, May 16-18, 1993.

43. "Program Result Checking: A New Approach to Making Programs More Reliable," Springer-Verlag Lecture Notes in Computer Science 700.

44. "Automata. Languages and Programming," ed. A. Lingas, R. Karlsson, and S. Carlsson, *ICALP 93,* 1-14.

45. “Self-testing/correcting with applications to numerical problems,” (with Michael Luby, and Ronitt Rubinfeld) *Journal of Computer and System Sciences,* 47(3), 549-595, December 1993.

46. "Matching Nuts and Bolts," (with Noga Alon, Amos Fiat, Sampath Kannan, Moni Naor, and Rafail Ostrovsky), *Proc. Symp. on Discrete Algorithms (SODA),* San Francisco, CA, January 15, 1994.

47. "Checking the Correctness of Memories" (with W. Evans, P. Gemmell, S. Kannan and M. Naor), *Algorithmica,* (ed. M. Blum and H. Wasserman), Vol. 12, 225-244, 1994.

48. "Program Result-Checking: A Theory of Testing Meets a Test of Theory," (with H. Wasserman), invited plenary lecture to *35th IEEE FOCS,* 382-393, 1995.

49. "On the Problem of Sorting Burnt Pancakes," (with D. Cohen), *Discrete Applied Mathematics,* Vol. 61,105-120, 1995.

50. "Reflections on the Pentium Division Bug," *IEEE Transactions on Computers.* Vol. 45, No 4, (April 1996), 385-393.

51. "Software Reliability Via Rtm-Time Result-Checking," (with Hal Wasserman), *JACM,* Vol. 44, No. 6, 826-849 (1997).

52. "Secure Human Identification Protocols" (with Nicholas J. Hopper), *ASIACRYPT 2001,* 52-66.

53. “On the complexity of MAX / MIN / AVRG Circuits,” (with Rachel Rue, Ke Yang). 2002. *CMU SCS Technical Report,* CMU-CS-02-110.

54. “CAPTCHA: Using Hard AI Problems for Security,” (with Luis von Ahn, Nicholas J. Hopper, and John Langford), *Advances in Cryptology - EUROCRYPT 2003,* Lecture Notes in *Computer Science 2656, Springer,* pp. 294 - 311, 2003. http://www.cs.cmu.edu/~biglou/captcha_crypt.pdf

55. “Telling Humans and Computers Apart Automatically: How Lazy Cryptographers do AI,” (with Luis von Ahn, Manuel Blum, and John Langford), *Communications of the ACM,* 47(2), 57-60, February 2004. http://www.cs.cmu.edu/~biglou/captcha_cacm.pdf

56. “Toward a High-level Definition of Consciousness,” (with Ryan Williams Brendan Juba, Matt Humphrey) . Invited Talk to the Annual *IEEE Computational Complexity Conference,* San Jose CA, (June 2005)

57. “Improving accessibility of the web with a computer game,” (with Luis von Ahn, Shiry Ginosar, Mihir Kedia, Ruoran Liu), *ACM CHI Notes,* 2006.

58. “Verbosity: A game for collecting common-sense facts,” (with Luis von Ahn and Mihir Kedia), “ *ACM CHI Notes,* 2006.

59. “Peekaboom: A game for locating objects in images,” (with Luis von Ahn and Ruoran Liu), *ACM CHI Notes,* 2006.

Ph.D. Students

1. Andy Kang, Research Scientist, consultant.

2. Tsun Chow, Faculty Chair of Information Technology Management, School of Business and Technology at Capella University. Former Research Scientist, Bell Laboratories.

3. Ion Filotti, Vice-president, DZ Consulting, France. Former Professor, Computer Science Department, Universite Paris Sud, Orsay, France.

4. Ivan Marques, Professor of the Mathematics Institute, Universidade Federal de Rio de Janeiro (UFRJ). Former Professor and Chairman, Computer Science Department, Federal University, Rio de Janeiro, Brazil.

5. John Gill, Professor, Electrical Engineering Department, Stanford University.

6. Ken Manders, Associate Professor, Dept. of Philosophy, University of Pittsburgh.

7. Leonard Adleman, Professor, Computer Science Department, University of Southern California.

8. Dana Angluin, Professor of Computer Science, Yale University.

9. Gary Miller, Professor, Computer Science Department, Carnegie Mellon University.

10. William Sakoda, Research Scientist, Symbol Technologies, Inc.. Former Professor, Computer Science Department, Penn State University.

11. Howard Katseff, Research Scientist, AT&T Labs Research, Florham Park, NJ.

12. Michael Sipser, Professor and Head, Mathematics Department, M.I.T.

13. Jeffrey Shallit , Professor, School of Computer Science, University of Waterloo.

14. Silvio Micali, Professor, EECS Department, M.I.T.

15. Shafi Goldwasser, Professor, EECS Department, M.I.T. and Weizmann Institute, Rehovat, Israel.

16. Joan Boyer (Plumstead), Associate Professor, Computer Science Department, University of Southern Denmark.

17. Vijay Vazirani, Professor, Computer Science Department, Georgia Institute of Technology.

18. Eric Bach, Professor, Computer Science Department, University of Wisconsin.

18. Rene Peralta, Computer Scientist, National Institute of Standards and Technology, Computer Security Division.

20. Umesh Vazirani, Professor, Department of Computer Science, University of California at Berkeley.

21. Steven Rudich, Professor, Department of Computer Science, Carnegie-Mellon University.

22. Moni Naor, Professor, Department of Computer Science, Weizmann Institute, Israel.

23. Russell Impagliazzo, Professor, Department of Computer Science, University of California at San Diego.

24. Sampath Kannan, Professor of Computer and Information Science, University of Pennsylvania.

25. Ronitt Rubinfeld, Professor, EECS Department, MIT.

26. Peter Gemmell, Professor of Computer Science, University of New Mexico.

27. William S. Evans, Associate Professor of Computer Science, University of British Columbia.

28. Mor Harchol-Balter, Associate Professor of Computer Science, Carnegie Mellon University.

29. Hal Wasserman, filmmaker and game designer.

30. Troy Shahoumian, Research Epidemiologist, Department of Veterans Affairs. Former, Research Scientist, Hewlett Packard, Palo Alto, CA.

31. Nicholas Hopper, Associate Professor, Computer Science & Engineering Department, University of Minnesota.

32. Luis von Ahn, Associate Professor of Computer Science, Carnegie Mellon University.

33. R. Ryan Williams, Assistant Professor of Computer Science, Stanford University.