

ANDREW CHI-CHIH YAO

1. Biographical and Personal Information

Born December 24, 1946, Shanghai, China.

Citizenship: U.S.A.

Mailing Address: Computer Science Department, Princeton University, Princeton, NJ 08544, USA

Email: yao@cs.princeton.edu

2. Education

National Taiwan University, B.S., Physics, 1967.

Harvard University, A.M., Physics, 1969; Ph.D., Physics, 1972.

University of Illinois, Ph.D., Computer Science, 1975.

3. Employment Record

Assistant Professor, Mathematics Department, Massachusetts Institute of Technology, 9/1975–8/1976.

Assistant Professor, Computer Science Department, Stanford University, 9/1976–8/1981.

Professor, Computer Science Division, University of California, Berkeley, 9/1981–9/1982.

Professor, Computer Science Department, Stanford University, 10/1982–6/1986.

William and Edna Macaleer Professor of Engineering and Applied Science, Computer Science Department, Princeton University, 7/1986–8/2004.

4. Other Positions

Military Service, Second Lieutenant in the Air Force, Republic of China, 7/1967–6/1968.

Research Associate, Physics Department, University of California, Santa Barbara, 7/1972–6/1973.

Visiting Scientist, IBM Research Center, Yorktown Heights, New York, Summer 1975.

Bell Laboratories, Murray Hill, New Jersey, 8/1978–12/1978.

Xerox Palo Alto Research Center, Palo Alto, California, 1/1979–6/1979.

IBM Research Center, San Jose, California, Summer 1980 and 1981, 9/1982–8/1983.

Consultant, DEC Systems Research Center, Palo Alto, California, 1/1986–6/1986.

AT & T Bell Laboratories, Murray Hill, New Jersey, 1/1991–12/1991.

Microsoft Research Asia, Beijing, China, 1/2003–present.

5. Research Interests

Analysis of Algorithms, Computational Complexity, Communication Complexity, Cryptographic Protocols, Quantum Computing.

6. Honors and Awards

George Polya Prize, Society for Industrial and Applied Mathematics, 1987.

Guggenheim Fellowship, 1991.

Fellow, Association for Computing Machinery, 1995.

Donald E. Knuth Prize, ACM SIGACT-IEEE TCMFCS, 1996.

Member, US National Academy of Sciences, 1998.

Fellow, American Academy of Arts and Sciences, 2000.

Member, Academia Sinica, 2000.

A.M. Turing Award, Association for Computing Machinery, 2000.

Pan Wen-Yuan Research Award, Pan Wen-Yuan Foundation, 2003.

Fellow, American Association for the Advancement of Science, 2003.

Doctor of Science, Honoris Causa, City University of Hong Kong, 2003.

Alumni Award for Distinguished Service, College of Engineering, University of Illinois, 2004.

Foreign Member, Chinese Academy of Sciences, 2004.

7. Editorial Boards

SIAM Journal on Computing, Managing Editor, 1989–1991.
Journal of Software, Associate Editor-in-Chief, 2001–present.
Journal of Combinatorial Optimization, Advisory Editor, 1997–present.
International Journal of Foundations of Computer Science, Advisory Board, 1994–present.
Algorithmica, 1985–present.
Information and Control, 1982–85.
Journal of ACM, 1982–83.
Journal of Algorithms, 1980–1991.
SIAM Journal on Computing, 1981–87.
Random Structures & Algorithms, 1990–2002.
Journal of Cryptology, 1991–1996.

8. Ph.D. Students, theses titles, and years of graduation:

Robert Scot Drysdale III, “Generalized Voronoi Diagrams and Geometric Searching,” 1978.
Kenneth L. Clarkson, “Algorithms for Closest-point Problems,” 1984.
Joan Feigenbaum, “Product Graphs: Some Algorithmic and Combinatorial Results,” 1986.
Oren Patashnik, “Optimal Circuit Segmentation for Pseudo-Exhaustive Testing,” 1990.
Wei-Zhen Mao, “Performance Bounds of Approximation Algorithms for Bin Packing,” 1990.
Hing-Fung Ting, “Computational Complexity for Selection Problems with Parity-Like Tests,” 1993.
Yaoyun Shi, “Lower Bounds for Quantum Decision Trees,” 2001.

9. Professional Activities

American Association for the Advancement of Science, member
Section Representative to AAAS for Section T (Computing), Conference Board of the Mathematical Sciences, 1981–84.
American Mathematical Society
Organizing Committee, AMS Workshop on Probabilistic Computational Complexity, New Hampshire, June 1982.
Association for Computing Machinery, member.
Program Committee, 10th Annual ACM Symposium on Theory of Computing, San Diego, 1978.
Program Committee, 2nd Annual ACM Symposium on Principles of Distributed Computing, Montreal, Canada, 1983.
Program Committee, 20th Annual ACM Symposium on Theory of Computing, Chicago, 1988.
Program Committee, 23rd Annual ACM Symposium on Theory of Computing, New Orleans, 1991.
Program Committee, 25th Annual ACM Symposium on Theory of Computing, San Diego, 1993.
Gödel Prize Committee (EATCS-SIGACT), Chair, 1993.
IEEE, member
Program Committee, 20th Annual IEEE Symp. on Found. of Computer Science, Puerto Rico, 1979.
Program Committee, Chairman, 21st Annual IEEE Symp. on Found. of Computer Science, Syracuse, 1980.
Program Committee, 36th Annual IEEE Symposium on Found. of Computer Science, Milwaukee, 1995.
Society for Industrial and Applied Mathematics
Visiting Lecturer, 1980–81.
George Polya Prize Committee, Chair, 1992.
George Polya Prize Committee, Member, 1998.
NSF DIMACS Center (Discrete Mathematics and Theoretical Computer Science)
Special Year in Complexity Theory, 9/1990-8/1991, Co-Organizer.
Co-Director, 6/1994-5/1996.

10. Publications

(see attached list)

Publications of Andrew C. C. Yao

1. “Divergences of Massive Yang-Mills Theories: Higher Groups,” (with S.L. Glashow and J. Iliopoulos), *Physical Review* **D4** (1971), 1918–1919.
2. “Standing Pion Waves in Superdense Matter,” (with R.F. Sawyer), *Physical Review* **D7** (1973), 1579–1586.
3. “An $O(|E| \log \log |V|)$ Algorithm for Finding Minimum Spanning Trees,” *Information Processing Letters* **4** (1975), 21–23.
4. “Analysis of the Subtractive Algorithms for Greatest Common Divisors,” (with D.E. Knuth), *Proceedings of the National Academy of Sciences USA* **72** (1975), 4720–4722.
5. “On Computing the Minima of Quadratic Forms,” *Proceedings of Seventh ACM Symposium on Theory of Computing*, Albuquerque, New Mexico, May 1975, 23–26.
6. “The Complexity of Non-uniform Random Number Generation,” (with D.E. Knuth), in *Algorithms and Complexity: New Directions and Recent Results*, edited by J.F. Traub, Academic Press, 1976, pp. 357–428.
7. “On the Evaluation of Powers,” *SIAM J. on Computing* **5** (1976), 100–103.
8. “Resource Constrained Scheduling as Generalized Bin Packing,” (with M.R. Garey, R.L. Graham, and D.S. Johnson), *J. of Combinatorial Theory* **A21** (1976), 257–298.
9. “Bounds on Merging Networks,” (with F.F. Yao), *Journal of ACM* **23** (1976), 566–571.
10. “Tiling with Incomparable Rectangles,” (with E.M. Reingold and W. Sanders), *Journal of Recreational Mathematics* **8** (1976), 112–119.
11. “A Combinatorial Optimization Problem Related to Data Set Allocation,” (with C.K. Wong), *Revue Francaise D’Automatique, Informatique, Recherche Operationnelle*, Suppl. No. **5** (1976), 83–96.
12. “On a Problem of Katona on Minimal Separation Systems,” *Discrete Mathematics* **15** (1976), 193–199.
13. “An Almost Optimal Algorithm for Unbounded Searching,” (with J. Bentley), *Information Processing Letters* **5** (1976), 82–87.
14. “On the Average Behavior of Set Merging Algorithms,” *Proceedings of Eighth ACM Symposium on Theory of Computing*, Hershey, Pennsylvania, May 1976, 192–195.
15. “The Complexity of Searching an Ordered Random Table,” (with F.F. Yao), *Proceedings of Seventeenth IEEE Symposium on Foundations of Computer Science*, Houston, Texas, October 1976, 222–227.
16. “Probabilistic Computations: Toward a Unified Measure of Complexity,” *Proceedings of Eighteenth IEEE Symposium on Foundations of Computer Science*, Providence, Rhode Island, October 1977, 222–227.
17. “On the Loop Switching Addressing Problem,” *SIAM J. on Computing* **7** (1978), 82–87.
18. “On Random 2–3 Trees,” *Acta Informatica* **9** (1978), 159–170.
19. “ $K + 1$ Heads are Better than K ,” (with R.L. Rivest), *Journal of ACM* **25** (1978), 337–340.
20. “Addition Chains with Multiplicative Cost,” (with R.L. Graham and F.F. Yao), *Discrete Mathematics* **23** (1978), 115–119.
21. “The Complexity of Pattern Matching for a Random String,” *SIAM J. on Computing* **8** (1979), 368–387.
22. “A Note on a Conjecture of Kam and Ullman Concerning Statistical Databases,” *Information Processing Letters* **9** (1979), 48–50.
23. “Storing a Sparse Table,” (with R.E. Tarjan), *Communications of ACM* **22** (1979), 606–611.
24. “On Some Complexity Questions in Distributive Computing,” *Proceedings of Eleventh ACM Symposium on Theory of Computing*, Atlanta, Georgia, May 1979, 209–213.
25. “External Hashing Schemes for Collections of Data Structures,” (with R.J. Lipton and A.L. Rosenberg), *Journal of ACM* **27** (1980), 81–95.
26. “New Algorithms for Bin Packing,” *Journal of ACM* **27** (1980), 207–227.

27. "Information Bounds are Weak for the Shortest Distance Problem," (with R.L. Graham and F.F. Yao), *Journal of ACM* **27**, (1980), 428–444.
28. "A Stochastic Model of Bin Packing," (with E.G. Coffman, Jr., M. Hofri, and K. So), *Information and Control* **44** (1980), 105–115.
29. "An Analysis of Shellsort," *Journal of Algorithms* **1** (1980), 14–50.
30. "On the Polyhedral Decision Problem," (with R.L. Rivest), *SIAM J. on Computing* **9** (1980), 343–347.
31. "Bounds on Selection Networks," *SIAM J. on Computing* **9** (1980), 566–582.
32. "Some Monotonicity Properties of Partial Orders," (with R.L. Graham and F.F. Yao), *SIAM J. on Algebraic and Discrete Methods* **1** (1980), 251–258.
33. "A Note on the Analysis of Extendible Hashing," *Information Processing Letters* **11** (1980), 84–86.
34. "Optimal Expected-Time Algorithm for Closest-point Problems," (with J.L. Bentley and B.W. Weide), *ACM Trans. on Math. Software* **6** (1980), 561–580.
35. "Efficient Searching via Partial Ordering," (with A. Borodin, L.J. Guibas and N.A. Lynch), *Information Processing Letters* **12** (1981), 71–75.
36. "An Analysis of a Memory Allocation Scheme for Implementing Stacks," *SIAM J. on Computing* **10** (1981), 398–403.
37. "Should Tables be Sorted?" *Journal of ACM* **28** (1981), 615–628.
38. "A Lower Bound for Finding Convex Hulls," *Journal of ACM* **28** (1981), 780–787.
39. "The Entropic Limitations on VLSI Computations," *Proceedings of Thirteenth ACM Symposium on Theory of Computing*, Milwaukee, Wisconsin, May 1981, 308–311.
40. "Average-case Complexity of Selecting the k -th Best," (with F.F. Yao), *SIAM J. on Computing* **11** (1982), 428–447.
41. "The Complexity of Finding Cycles in Periodic Functions," (with R. Sedgewick and T.G. Szymanski), *SIAM J. on Computing* **11** (1982), 376–390.
42. "On the Time-Space Tradeoff for Sorting with Linear Queries," *Theoretical Computer Science* **19** (1982), 203–218.
43. "Lower Bounds to Algebraic Decision Trees," (with J.M. Steele, Jr.), *Journal of Algorithms* **3** (1982), 1–8.
44. "On Parallel Computation for the Knapsack Problem," *Journal of ACM* **29** (1982), 898–903.
45. "On Constructing Minimum Spanning Trees in k -dimensional Spaces and Related Problems," *SIAM J. on Computing* **11** (1982), 721–736.
46. "Equal justice for unequal shares of the cake," (with M. Klawe), *Congressus Numerantium* **36** (1982), 247–260.
47. "Rearrangeable networks with limited depth," (with N. Pippenger), *SIAM J. on Algebraic and Discrete Methods* **3** (1982), 411–417.
48. "Space-Time Tradeoff for Answering Range Queries," *Proceedings of Fourteenth ACM Symposium on Theory of Computing*, San Francisco, California, May 1982, 128–136.
49. "Theory and Applications of Trapdoor Functions," *Proceedings of Twenty-third IEEE Symposium on Foundations of Computer Science*, Chicago, Illinois, November 1982, 80–91.
50. "Protocols for Secure Computations," *Proceedings of Twenty-third IEEE Symposium on Foundations of Computer Science*, Chicago, Illinois, November 1982, 160–164.
51. "On the Security of Public Key Protocols," (with D. Dolev), *IEEE Trans. on Information Theory* **29** (1983), 198–208.
52. "Strong Signature Schemes," (with S. Goldwasser and S. Micali), *Proceedings of Fifteenth ACM Symposium on Theory of Computing*, Boston, Massachusetts, April 1983, 431–439.
53. "Lower Bounds by Probabilistic Arguments," *Proceedings of Twenty-fourth IEEE Symposium on Foundations of Computer Science*, Tucson, Arizona, November 1983, 420–428.

54. “Context-free Grammars and Random Number Generation,” *Proceedings of NATO Workshop on Combinatorial Algorithms on Words*, Maratea, Italy, July 1984, edited by A. Apostolico and Z. Galil, Academic Press, 357–361.
55. “Fault-tolerant Networks for Sorting,” (with F.F. Yao), *SIAM J. on Computing* **14** (1985), 120–128.
56. “On the Expected Performance of Path Compression,” *SIAM J. on Computing* **14** (1985), 129–133.
57. “On Optimal Arrangements of Keys with Double Hashing,” *Journal of Algorithms* **6** (1985), 253–264.
58. “Uniform Hashing is Optimal,” *Journal of the ACM* **32** (1985), 687–693.
59. “On the Complexity of Maintaining Partial Sums,” *SIAM J. on Computing* **14** (1985), 253–264.
60. “A General Approach to d -dimensional Geometric Queries,” (with F.F. Yao), *Proceedings of Seventeenth ACM Symposium on Theory of Computing*, Providence, Rhode Island, May 1985, 163–168.
61. “Separating the Polynomial-time Hierarchy by Oracles,” *Proceedings of Twenty-sixth IEEE Symposium on Foundations of Computer Science*, Eugene, Oregon, October 1985, 1–10.
62. “How to Generate and Exchange Secrets,” *Proceedings of Twenty-seventh IEEE Symposium on Foundations of Computer Science*, Toronto, Canada, October 1986, 162–167.
63. “Monotone Bipartite Graph Properties are Evasive,” *SIAM J. on Computing* **17** (1988), 517–520.
64. “Computational Information Theory,” in *Complexity in Information Theory*, edited by Y. Abu-Mostafa, Springer-Verlag, 1988, 1–15.
65. “Selecting the k Largest with Median Tests,” *Algorithmica* **4** (1989), 293–300.
66. “On the Complexity of Partial Order Productions,” *SIAM J. on Computing* **18** (1989), 679–689.
67. “On the Improbability of Reaching Byzantine Agreement,” (with R.L. Graham) *Proceedings of Twenty-First ACM Symposium on Theory of Computing*, Seattle, Washington, May 1989, 467–478.
68. “Circuits and Local Computations,” *Proceedings of Twenty First ACM Symposium on Theory of Computing*, Seattle, Washington, May 1989, 186–196.
69. “Computing Boolean Functions with Unreliable Tests,” (with C. Kenyon-Mathieu) *International Journal of Foundations of Computer Science*, **1** (1990), 1–10.
70. “Coherent Functions and Program Checkers,” *Proceedings of Twenty-second ACM Symposium on Theory of Computing*, Baltimore, Maryland, May 1990, 84–94.
71. “On ACC and Threshold Circuits,” *Proceedings of Thirty-first IEEE Symposium on Foundations of Computer Science*, October 1990, 619–627.
72. “Lower Bounds to Randomized Algorithms for Graph Properties,” *Journal of Computer and System Sciences* **42** (1991), 267–287.
73. “Lower Bounds for Algebraic Computation Trees with Integer Inputs,” *SIAM J. On Computing* **20** (1991), 655–668.
74. “Program Checkers for Probability Generation,” (with S. Kannan) *Proceedings of Eighteenth International Colloquium on Automata, Languages and Programming*, Madrid, Spain, July 1991, 163–173.
75. “Linear Decision Trees: Volume Estimates and Topological Bounds,” (with A. Björner and L. Lovász) *Proceedings of Twenty-fourth ACM Symposium on Theory of Computing*, May 1992, 170–177.
76. “A Circuit-Based Proof of Toda’s Theorem,” (with R. Kannan, H. Venkateswaran, and V. Vinay) *Information and Computation* **104** (1993), 271–276.
77. “Towards Uncheatable Benchmarks,” (with J. Cai, R. Lipton, and R. Sedgewick) *Proceedings of Eighth IEEE Annual Structure in Complexity Conference*, San Diego, California, May 1993, 2–11.
78. “Quantum Circuit Complexity,” *Proceedings of Thirty-fourth IEEE Symposium on Foundations of Computer Science*, Palo Alto, California, November 1993, 352–361.
79. “A Randomized Algorithm for Maximum Finding with Parity Tests,” (with H.F. Ting), *Information Processing Letters* **49** (1994), 39–43.
80. “Near-Optimal Time-Space Tradeoff for Element Distinctness,” *SIAM J. On Computing*, **23** (1994), 966–975.

81. "A Lower Bound for the Monotone Depth of Connectivity," *Proceedings of Thirty-fifth IEEE Symposium on Foundations of Computer Science*, Santa Fe, New Mexico, November 1994, 302–308.
82. "On Computing Algebraic Functions Using Logarithms and Exponentials," (with D. Grigoriev and M. Singer) *SIAM J. on Computing* **24** (1995), 242–246.
83. "Algebraic Decision Trees and Euler Characteristics," *Theoretical Computer Science* **141** (1995), 133–150.
84. "On the Shrinkage Exponent for Read-Once Formulae," (with J. Hastad and A. Razborov), *Theoretical Computer Science*, **141** (1995), 269–282.
85. "Minimean Optimal Key Arrangements in Hash Tables," *Algorithmica* **14** (1995), 409–428.
86. "Security of Quantum Protocols Against Coherent Measurements," *Proceedings of Twenty-seventh ACM Symposium on Theory of Computing*, Las Vegas, Nevada, May 1995, 67–75.
87. "Decision Tree Complexity and Betti Numbers," *Journal of Computer and Systems Sciences*, **55** (1997), 36–43.
88. "Dictionary Look-Up with One Error," (with F. Yao), *Journal of Algorithms*, **25** (1997), 194–202.
89. "Read-Once Branching Programs, Rectangular Proofs of the Pigeonhole Principle and the Transversal Calculus," (with A. Razborov and A. Wigderson), *Proceedings of Twenty-ninth ACM Symposium on Theory of Computing*, May 1997, 739–784.
90. "RAPID: Randomized Pharmacophore Identification for Drug Design," (with L. Kaviraki, J. Latombe, R. Motwani, C. Shelton, and S. Venkatasubramanian), *Proceedings of 1997 ACM Symposium on Applied Computational Geometry*, Nice, France, 1997, 324–333.
91. "A Lower Bound on the Size of Algebraic Decision Trees for the MAX Problem," (with D. Grigoriev and M. Karpinski), *Computational Complexity* **7** (1998), 193–203.
92. "Quantum Cryptography with Imperfect Apparatus," (with D. Mayers), *Proceedings of Thirty-ninth IEEE Symposium on Foundations of Computer Science*, October 1998, 503–509.
93. " $NQP_C = co - C = P$," (with T. Yamakami), *Information Processing Letters*, **71** (1999), 63–69.
94. "Quantum Bit Escrow," (with A. Aharonov, A. Ta-Shma and U. Vazirani), *Proceedings of Thirty-second ACM Symposium on Theory of Computing*, May 2000, 715–724.
95. "Informational Complexity and the Direct Sum Problem for Simultaneous Message Complexity," (with A. Chakrabarti, Y. Shi, and A. Wirth), *Proceedings of Forty-second IEEE Symposium on Foundations of Computer Science*, October 2001, 270–278.
96. "Classical Physics and the Church-Turing Thesis," *Journal of ACM* **50** (2003), 100–105.
97. "On the Power of Quantum Fingerprinting," *Proceedings of Thirty-fifth ACM Symposium on Theory of Computing*, June 2003, 77–81.
98. "Graph Entropy and Quantum Sorting Problems," to appear in *Proceedings of Thirty-sixth ACM Symposium on Theory of Computing*, June 2004.
99. "Incentive Compatible Price Sequence in Dynamic Auctions," (with N. Chen, X. Deng, and X. Sun), to appear in *Proceedings of Thirty-first International Colloquium on Automata, Languages and Programming*, Turku, Finland, July 2004.
100. "Market Equilibrium with a Class of Concave Utility Functions," (with N. Chen, X. Deng, and X. Sun), to appear in *Proceedings of 12th Annual European Symposium on Algorithms*, Bergen, Norway, September 2004.