# RESUME: Shimon EVEN

May 14, 2001

## Personal Data


| | |
|---|---|
| Date of Birth: | June 15, 1935 |
| Place of Birth: | Ramat Gan, Israel |
| Family Status: | Married + 3 |
| Citizenship: | Israeli |
| Telephone: | Home +972 4 824 1747 Office +972 4 829 4166 |
| Fax: | +972 4 822 1128 |
| E-address: | even@cs.technion.ac.il |


## Academic Degrees

| | |
|---|---|
| 1959 | B.A. in Electrical Engineering (Summa cum Laude) - Technion-IIT, Haifa, Israel. |
| 1961 | M.A. in Mathematics - University of North Carolina, Chapel Hill, N.C., USA. |
| 1963 | Ph.D. in Applied Mathematics - Harvard University, Cambridge, Mass., USA. |

## Employment

| | |
|---|---|
| 1959-60 | Laboratory Assistant and Research Engineer, University of North Carolina, Chapel Hill, N.C. |
| 1961-62 | Teaching Fellow and Research Assistant, Harvard University, Cambridge, Mass. |
| 1963-64 | Research Staff Member, Sperry-Rand Research Center, Sudbury, Mass. Also a Lecturer in Applied Mathematics, Harvard University, Cambridge, Mass. |
| 1964-67 | Lecturer, Department of Mathematics, Technion, Haifa, Israel. Promoted to Senior Lecturer in October 1965. Also, consultant to the Elron and Elbit Electronic Industries. |
| 1967-69 | Visiting Professor, Harvard University. Also, consultant to Sperry-Rand Research Center, Sudbury, Mass. |
| Summer 1969 | Research summer employment with Computer Associates, New York. |
| 1969-74 | Associate Professor, The Weizmann Institute of Science. Founded and headed the teaching program in Computer Science. |
| Summer 1971 | Research summer employment with Sperry-Rand Research Center, Sudbury, Mass. |
| Summ. 1972 & Summ. 1973 | |

| | |
|---|---|
| | Visiting research appointment in the Dept. of Computer Science, Cornell University, N.Y. |
| Oct. 1974 to present | Professor of Computer Science, Technion, Haifa, Israel. |
| Summer 1976 | Visiting research appointment, Laboratory for Computer Science, MIT, Cambridge, Mass. |
| 1976-77 | Visiting Professor, Computer Science Division-EECS, University of California, Berkeley, CA. |
| July 1977 | Visiting research appointment, Computer Science Dept., Stanford University, Stanford, CA. |
| August 1977 | Visiting research appointment, Bell Laboratories, Murray Hill, N.J. |
| July 1978 | Teaching a course on Graph Algorithms, Summer school, (C.N.R.), Lecce, Italy. |
| Sept. 1978 & Sept. 1980 | Visitor, Mathematical Institute, Technical University of Denmark, Lyngby, Denmark. |
| 1979-80, 1986-89 | Chairman, Computer Science Dept., Technion, Haifa, Israel. |
| July-Aug. 1979 | Visitor, E.E. Dept., University of Southern California, Los Angeles, CA. |
| Sept. 1979, Aug. 1980, Summers 1981, 1982, 1983 | Visitor, Dept. of EECS, University of California, Berkeley, CA. |
| 1981-83, 1993-96 | Member of the Technion's Central Committee. |
| Aug.-Dec. 1983 | Visiting Professor, Dept. of EECS, University of California, Berkeley, CA. |
| Mar.-Sep. 1984 | Visiting Professor, Dept. of CS, Univ. of Chicago, Chicago, IL. |
| Jan.-May 1985 | Visiting Professor, Dept. of CS, Duke Univ., Durham, NC. |
| Jul.-Aug. 1986 | Visiting Professor, Dept. of CS, Univ. of Salerno, Salerno, Italy. |
| Aug.-Sep. 1988 | Visiting Professor, Fachbereich Mathematik und Informatik, Universitat Gesamthochschule Paderborn, Paderborn, West Germany. |
| Aug.-Dec. 1989 | Visiting Professor, Comp. Sci. Program, Univ. of Texas at Dallas, Richardson, TX. |
| Dec. 1989 | Visitor, Laboratory for Computer Science, MIT. |
| Jan.-Sep. 1990, July-Sep. 1991 | Visitor, Bellcore, Morristown, NJ. |
| July 1992 | Visitor, UNAM, Mexico City. |
| Aug. 1992 | Visiting Professor, Dept. of CS, Boston University, Boston, MA. |
| Aug. 1996 -Sep. 1997, Aug.-Sep. 1998 | Visitor, Bell-Labs, Lucent Technologies, Murray Hill, NJ. |

## Positions in International Conferences and Journals

| | |
|---|---|
| 1977-present | Member of the advisory board of the EATCS Monographs on Theoretical Computer Science |
| 1980-83, 1987, 1992 | ICALP Program committee member. Program Chairman, ICALP '81. |
| 1980-present | Journal of Algorithms, member of the Editorial Board. |
| 1979-87 | Discrete Applied Mathematics, member of the Editorial Board. |
| 1984 | Member of program committee, FOCS. |
| 1988-present | Theory of Computing Systems, member of the Editorial Board. |
| 1991 | Member of program committee, AsiaCrypt. |

| | |
|---|---|
| 1992 | Member of program committee,<br>Algorithms and Efficient Computation Stream, IFIP. |
| 1993 | Co-Chairman of ISTCS '93. |
| 1993-present | Member of the Steering Committee, ISTCS |
| 1993, 1999 | Member of program committee,<br>Italian Conference on Algorithms and Complexity. |
| 1994 | Member of program committee, CRYPTO. |
| 1995-present | Member of the advisory board,<br>Journal of Graph Algorithms and Applications. |
| 1996 | Member of program committee, ISTCS. |
| 1997 | Member of program committee, STOC. |

### Prizes and grants

| | |
|---|---|
| 1955-59 | The Fischbach Scholarship. |
| 1981 | The George Farkas Chair in Computer Science. |
| 1982 | A Technion outstanding teacher award, for the Cryptology course |
| 1992 | The Henry Taub Prize in Computer Science. |
| 1994 | ETH Distinguished Lecturers Series. |
| 1995-98 | A United States-Israel Binational Science Foundation<br>grant No. 94-00266/1 (joint with Y. Dinitz, A. Litman and A.L. Rosenberg). |
| 1995 | Keynote speaker, ESA '95. |
| 1996 | Salomon Simon Mani Award for Excellence in Teaching. |
| 1997 | Invited speaker, CIAC '97 |

### Fields of Interest

Applications of Combinatorics and Graph Theory to Computer Science, with emphasis on algorithms and their complexity. Circuit layout. Distributed, parallel and systolic systems. Cryptography.

### PAPERS

1. An Analysis of Logical Design using the Field of Integers Modulo 2, Mathematical Note, No.6, Computation Center, University of North Carolina. Summary of the paper was presented in the ACM National Conference, Milwaukee, Wisconsin (1960), (M.A. thesis).

2. An Extension of Linear Sequential Machines, SRRC-RR-615 (1961).

3. Binary and Generalized Dagger and Stroke Forms for Boolean Functions, Report No. BL-320 of the Comp. Lab. of Harvard University, January 1962. A portion of this paper was published as a note in the *IRE Trans. on Circuit Theory* entitled "On the Correspondence between Simplest Disjunctive and Conjunctive Forms and Simplest Stroke and Dagger Functions", Vol.8, No.4, December 1961, p.489.

4. (with M. Cohn, K. Menger and P.K. Hooper) On the Number of Partitionings of a Set of $n$ Distinct Objects, *Amer. Math. Monthly*, Vol.69, No.8, October 1962, pp. 782-785.

5. On Information Lossless Automata of Finite Order, Proc. of International Symp. on Theory of Relay Systems and Finite Automata, Moscow, USSR, Sept. 1962 (Russian). A revised version appeared in *IEEE Trans. on Elect. Comp.*, Vol. EC-14, No.4, August 1965, pp. 561-569.

6. Generalized Automata and their Information Losslessness, Proc. AIEE Ann. Symp. on Switching Circuit Theory and Logical Design (now FOCS), Chicago, Illinois, October 7-12, 1962, pp. 143-147.

7. Snake in the Box Codes, *IEEE Trans. on Elect. Comp.*, Vol. EC-123, No.1, 1963, p. 18.

8. Determination of Automaton Memory, SRRC-RR-63-51 (1963).

9. The Prefix and Suffix of One Regular Event with Respect to Another, SRRC-RR-63-55 (1963).

10. Machines whose Inputs are Restricted by a Regular Event, SRRC-RR-63-59 (1963).

11. Test for Unique Decipherability, *IEEE Trans. on Information Theory*, Vol. IT-9, No.2, April 1963, pp. 109-112.

12. Test of Synchronizability of Finite Automata and Variable Length Codes, *IEEE Trans. on Inf. Theory*, Vol. IT-10, No.3, July 1964, pp. 185-189.

13. (with W.L. Eastman) On Synchronizability and PSK-Synchronizable Block Codes, *IEEE Trans. on Inf. Theory*, Vol. IT-10, October 1964, pp. 351-356.

14. (with W.L. Eastman and I.M. Isaacs) Bounds for the Optimal Scheduling of $n$ Jobs on $m$ Processors, *Management Science*, Vol.11, No.2, November 1964, pp. 268-279.

15. Rational Numbers and Regular Events, *IEEE Trans. on Elect. Comp.*, Vol. EC-13, No.6, December 1964, pp. 740-741.

16. Comments on the Minimization of Stochastic Machines, *IEEE Trans. on Elect. Comp.*, Vol. EC-14, No.4, August 1965, pp. 634-637.

17. (with M. Cohn) Identification and Minimization of Linear Machines, *IEEE Trans. on Elect. Comp.*, Vol. EC-14, No.3, June 1965, pp. 367-376.

18. 'The Price is Right' Game, *Amer. Math. Monthly*, Vol. 73, No.2, February 1966, pp. 180-182.

19. (with A.R. Meyer), Test for Planarity of a Circuit Given by an Expression, *IEEE Trans. on Elect. Comp.*, Vol. EC-15, No.3, June 1966, pp. 372-375.

20. (with W.L. Eastman) Some Further Results on Synchronizable Block Codes, *IEEE Trans. on Information Theory*, Vol. IT-12, No.3, July 1966, pp. 405-406.

21. (with A. Lempel and I. Cederbaum) An Algorithm for Planarity Testing of Graphs, *Theory of Graphs, International Symposium*, Rome 1966, Gordon and Breach, N.Y., 1967, pp. 215-232.

22. (with I. Kohavi and A. Paz) On Minimal Modulo 2 Sums of Products for Switching Functions, *IEEE Trans. on Elect. Comp.*, Vol. EC-16, No.5, October 1967, pp. 671-674.

23. (with A. Lempel) On a Problem of Diagnosis, *IEEE Trans. on Circuit Theory*, Vol. CT-14, No.3, September 1967, pp. 361-364.

24. (with A.R. Meyer) Sequential Boolean Equations, *IEEE Trans. on Elect. Comp.*, Vol. C-18, No.3, March 1969, pp. 230-240.

25. (with M. Cohn) The Design of Shift Register Generators for Finite Sequences, *IEEE Trans. on Elect. Comp.*, Vol. C-18, No.7, July 1969, pp. 660-662.

26. (with M. Cohn) A Gray Code Counter, *IEEE Trans. on Elect. Comp.*, Vol C-18, No.7, July 1969, pp. 662-664.

27. (with F. Brioschi) Minimizing the Number of Operations in Certain Discrete Variable Optimization Problems, *Operations Research*, Vol. 18, No.1, January 1970, pp. 66-81.

28. (with R. Book, S. Greibach and G. Ott) Ambiguity in Graphs and Expressions, *IEEE Trans. on Computers*, Vol. C-20, No.2, February 1971, pp. 149-153.

29. Codes for Magnetic Recording, SRRC-RR-31, July 1969. Was classified by Sperry Rand as proprietary information, and was not allowed to be published.

30. (with A.J. Lincoln and M. Cohn) Smooth Pulse Sequences, Proceedings of the 3rd Annual Princeton Conference on Information Sciences and Systems, 1969, pp. 350-354.

31. (with M. Cohn, S. Golomb and A. Lempel) The Stability of Counting Sequences under Stage Delays, *SIAM J. Appl. Math.*, Vol. 20, o.2, March 1971, pp. 183-188.

32. (with A. Lempel and A. Pnueli) Permutation Graphs and Transitive Graphs, *J. of ACM*, Vol. 19, No.3, July 1972, pp. 400-410.

33. (with A. Lempel and A. Pnueli) Transitive Orientation of Graphs and Identification of Permutation Graphs, *Canadian J. of Mathematics*, Vol. 23, No.1, 1971, pp. 160-175.

34. (with F. Commoner, A.W. Holt and A. Pnueli) Marked Directed Graphs, *Journal of Computer and System Sciences*, Vol.5, October 1971, pp. 511-523.

35. (with A. Itai) Queues, Stacks and Graphs, *Theory of Machines and Computations*, Z. Kohavi and A. Paz (eds.), Academic Press, 1971, pp. 71-86.

36. (with A. Lempel and M. Cohn) An Algorithm for Optimal Prefix Parsing of a Noiseless and Memoryless Channel, *IEEE Trans. on Inform. Theory*, Vol. IT-19, No.2, March 1973, pp. 208-214.

37. (with A. Lempel) Generation and Enumeration of all Solutions of the Characteristic Sum Condition, *Inform. and Control*, Vol. 21, No.5, December 1972, pp. 476-482.

38. Parallelism in Tape-Sorting, *Comm. of the ACM*, April 1974, Vol. 17, No.4, pp. 202-204.

39. (with Y. Perl and M.R. Garey) Efficient Generation of Optimal Prefix Code - Equiprobable Words Using Unequal Cost Letter, *J. of the ACM*, Vol. 22, No.2, April 1975, pp. 202-214.

40. (with G. Ehrlich and R.E. Tarjan) Intersection Graphs of Curves in the Plane, *J. of Combinatorial Th. (B)*, Vol. 21, No.1, August 1976, pp. 8-12.

41. An Algorithm for Determining whether the Connectivity of a Graph is at least $k$. *SIAM J. on Computing*, Vol. 4, No.3, September 1975, pp. 393-396.

42. (with R.E. Tarjan) Network Flow and Testing Graphs Connectivity, *SIAM J. on Computing*, Vol. 4, No.4, December 1975, pp. 507-508.

43. (with A. Shamir and A. Itai) On the Complexity of Timetable and Integral Multi-Commodity Flow Problems, *SIAM J. on Computing*, Vol. 5, No.4, December 1976, pp. 691-703.

44. (with Y. Shiloach) NP-Completeness of Several Arrangement Problems, TR#43, Dept. of Computer Science, Technion, January 1975.

45. (with O. Kariv) An $0(n^{2.5})$ Algorithm for Maximum Matching in General Graphs, 16th Ann. Symp. on Found. of Comp. Sci., October 1975, pp. 100-112.

46. (with J. Gillis) Derangements and Laguerre Polynomials, *Math. Proc. Camb. Phil. Soc.*, Vol. 79, 1976, pp. 135-143.

47. (with R.E. Tarjan) Computing an ST Numbering, *Theoretical Computer Science*, Vol. 2, 1976, pp. 339-344.

48. (with R.E. Tarjan) A Combinatorial Problem which is Complete in Polynomial Space, *J. of the ACM*, Vol. 23, No.4, 1976, pp. 710-719.

49. (with M. Rodeh) Economical Encoding of Commas Between Strings, *J. of the ACM*, Vol. 21, No.4, April 1978, pp. 315-317.

50. (with Y. Shiloach) An On-Line Edge-Deletion Problem, *J. of the ACM*, Vol. 28, No.1, January 1981, pp. 1-4.

51. (with M. Rodeh and V. Pratt) Linear Algorithm for Data Compression via String Matching, *J. of the ACM*, Vol. 28, No.1, January 1981, pp. 16-24.

52. (with Y. Yacobi) Cryptocomplexity and NP-Completeness, Proc. of ICALP 80, Noordwijkerhout, July 1980, Lecture Notes in Computer Science, Vol. 85, Springer-Verlag, 1980, pp. 195-207.

53. (with Y. Yacobi) An Observation Concerning the Complexity of Problems with Few Solutions and its Application to Cryptography, Graphtheoretic Concepts in Computer Science, (Proceedings of the International Workshop WG80, June 15-18, 1980, Bad Honnef). *Lecture Notes in Computer Science*, Vol. 100, Springer-Verlag, 1981, pp. 270-278.

54. (with Y. Yacobi) Relations among Public Key Signature Problems, TR#175, Computer Science Dept., Technion, March 1980.

55. (with R. Bar-Yehuda) A Linear-Time Approximation Algorithm for the Weighted Vertex Cover Problem, *J. of Algorithms*, Vol. 2, June 1981, pp. 198-203.

56. (with A.L. Selman and Y. Yacobi) Hard-Core Theorems for Complexity Classes, *J. of the ACM*, Vol. 32, No. 1, Jan. 1985, pp. 205-217.

57. (with R. Bar-Yehuda) On Approximating a Vertex Cover for Planar Graphs, Proceedings of the 14th Ann. ACM Symp. on Th. of Computing, San Francisco, CA, May 1982, pp. 303-309.

58. (with O. Goldreich) The Minimum Length Generator Sequence Problem is NP-Hard, *J. of Algorithms*, Vol. 2, September 1981, pp. 311-313.

59. (with T.J. Long and Y. Yacobi) A Note on Deterministic and Nondeterministic Time Complexity, *Information and Control*, Vol. 55, 1982, pp. 117-124.

60. (with A. Paz) A Note on Cake Cutting, *Discrete App. Math.*, Vol. 7, 1984, pp. 285-296. [Contains the paper: "On the Protocols for Fair Cake Cutting", which appeared in Proc. of the 7th Conf. on Graphtheoretic Concepts in Computer Science (WG81), J.R. Muhlbacher (ed.), Hanser Verlag, 1982, pp. 183-193.]

61. (with O. Goldreich) DES-Like Functions can Generate the Alternating Group, *IEEE Trans. on Infor. Th.*, Vol. IT-29, No. 6, November 1983, pp. 863-865.

62. (with O. Goldreich, P. Tong and S. Moran) On the NP-Completeness of Certain Network-Testing Problems, *Networks*, Vol. 14, No. 1, 1984, pp. 1-24.

63. A Protocol for Signing Contracts, in Advances in Cryptography, (A Report on CRYPTO81,) A.G. Gersho (ed.). ECE Rept. No. 82-04, University of California, Santa Barbara, pp. 148-153.

64. (with O. Goldreich and A. Lempel) A Randomized Protocol for Signing Contracts, *Comm. of the ACM*, Vol. 28, No. 6, 1985, pp. 637-647. [An extended abstract appeared in Advances in Cryptology: Proceedings of CRYPTO82, D. Chaum et al (eds.), Plenum Press, 1983, pp. 205-210.]

65. (with D. Dolev and R.M. Karp) On the Security of Ping-Pong Protocols, *Information and Control*, Vol. 55, 1982, pp. 57-68.

66. (with A. Selman and Y. Yacobi) The Complexity of Promise Problems with Applications to Public-Key Cryptography, *Information and Control*, Vol.61, No. 2, May 1984, pp. 159-173.

67. (with R. Bar-Yehuda) A Local-Ratio Theorem for Approximating the Weighted Vertex Cover Problem, *Annals of Discrete Math.*, Vol. 25, 1985, pp. 27-46.

68. (with O. Goldreich) On the Security of Multi-Party Ping-Pong Protocols, 24th Annual Symp. on Foundations of Computer Science, IEEE Computer Society, November 1983, pp. 34-39.

69. (with O. Goldreich) On the Power of Cascade Ciphers, *ACM Trans. on Computer Systems*, Vol. 3, No. 2, 1985, pp. 108-116.

70. (with O. Goldreich and Y. Yacobi) Electronic Wallet, Advances in Cryptology: Proc. of Crypto 83, D. Chaum (ed), Plenum Press, 1984, pp. 383-386.

71. (with B. Awerbuch) Reliable Broadcast Protocols in Unreliable Networks, *Networks*, Vol. 16, 1986, pp. 381-396. [A fuller version: A Formal Approach to a Communication-Network Protocol; Broadcast as a Case Study, PUB No. 459, Dept. of Elec. Eng., Technion-IIT, December 1983.]

72. (with H. Gazit) Updating Distances in Dynamic Graphs, *Methods of Operations Research*, Vol. 49, May 1985, pp. 371-387.

73. On the Complexity of Some Word Problems That Arise in Testing the Security of Protocols, in *NATO Advanced Research Workshop on Combinatorial Algorithms on Words, (1984: Maratea, Italy)*, Alberto Apostolico and Zvi Galil, editors, Springer-Verlag, Series F: Computer and System Sciences, Vol. 12, pp. 299-314.

74. (with O. Goldreich and A. Shamir) On the Security of Ping-Pong Protocols Using the RSA, in Advances in Cryptology - Proc. Crypto 85, pp. 58-72, 1985.

75. Secure Off-Line Electronic Fund Transfer Between Nontrusting Parties, *Smart Card 2000: The future of IC cards*, D. Chaum and I. Schaumuller-Bichl (eds.), North-Holland 1989, pp. 57-66.

76. (with Y. Pnueli) How to Keep a Dynamic Distributive Directed Graph Acyclic and Yet Grant All Requests of Edge Additions, *The 5th Jerusalem Conference on Information Technology (JCIT)*, IEEE 1990, pp. 414-425. [Fuller version in Technical Report #604, Dept. of Comp. Sci., Technion, Jan. 1990.]

77. (with S. Rajsbaum) Unison, Canon and Sluggish Clocks in Networks Controlled by a Synchronizer. *Math. Sys. Th.*, Vol. 28, 1995, pp. 421-435. [Includes the paper: Unison in Distributed Networks, in *Sequences, Combinatorics, Compression, Security and Transmission*, R.M. Capocelli (ed.), Springer-Verlag, 1990, pp. 479-487.]

78. (with B. Monien) On the Number of Rounds Necessary to Disseminate Information, *Proceedings of the 1989 ACM Symp. on Parallel Algorithms and Architectures*, June 18-21, 1989, Santa Fe, New Mexico, ACM, pp. 318-327.

79. (with O. Goldreich and S. Micali) On-Line/Off-Line Digital Signatures, *Journal of Cryptology*, Vol. 9, No. 1, 1996, pp. 35-67.

80. (with S. Rajsbaum) The Use of a Synchronizer Yields Maximum Computation Rate in Distributed Networks, *Theory of Computing Systems*, Vol. 30, 1997, pp. 447-474. [Also in the *Proceedings of the 22-nd Annual ACM Symp. on Theory of Computing*, Baltimore, Maryland, May 14-16, 1990, ACM 1990, pp. 95-105.]

81. (with A. Litman and P. Winkler) Computing with Snakes in Directed Networks of Automata, *Journal of Algorithms*, Vol. 24, 1997, pp. 158-170. [Also in *Proceedings of the 31-st Symp. on Foundations of Comp. Sci*, IEEE 1990, pp. 740-745.]

82. Systolic Modular Multiplication, *Advances in Cryptology - CRYPTO'90 Proceedings*, A.J. Menezes and S.A. Vanstone (eds.), Lecture Notes in Comp. Sci., Vol 537, Springer-Verlag 1991, pp. 619-624.

83. (with A. Litman) On the Capabilities of Systolic Systems. *Math. Sys. Th.*, Vol. 27, 1994, pp. 3-28.

84. (with Y. Mansour) A Construction of a Pseudorandom Cipher from Single Pseudorandom Permutation. *Journal of Cryptology*, Vol. 10, 1997, pp. 151-161. [Also in *Advances in Cryptology - ASIACRYPT'91*, H. Imai et.al. (eds.). Lecture Notes in Comp. Sci., Vol. 739, Springer-Verlag 1993, pp. 210-224.]

85. (with A. Litman) A Systematic Design and Explanation of the Atrubin Multiplier. In *Sequences II, Methods in Communication, Security and Computer Sciences*, R. Capocelli et.al. (Editors), Springer-Verlag 1993, pp. 189-202.

86. (with A. Litman) Layered Cross Product - A Technique to Construct Interconnection Networks, *Networks*, Vol. 29, 1997, pp. 219-223. [Also in the proceedings of the *4th Annual ACM Symposium on Parallel Algorithms and Architectures*, ACM Press 1992, pp. 60-69. Invited talk in IWIN'95, Luminy, France, June 1995.]

87. (with A. Litman) A Unified Scheme for Routing in Expander Based Networks. *Algorithms and Complexity.* Proceedings of CIAC'94. M. Bonuccelli et.al. (eds.). Lecture Notes in Comp. Sci., Vol. 778, Springer-Verlag 1994, pp. 125-135.

88. (with G. Granot) Rectilinear Planar Drawings with Few Bends in Each Edge. Technical Report #797, Jan. 1994, Technion, Department of Computer Science.

89. (with G. Granot) Grid Layout of Block Diagrams – Bounding the Number of Bends in Each Connection. In *Graph Drawing*, R. Tamassia and I.G. Tollis (eds.). Lecture Notes in Comp. Sci., Vol. 894, Springer-Verlag 1995, pp. 64-75.

90. (with A. Litman and A.L Rosenberg) Monochromatic Paths and Triangulated Graphs, *SIAM J. on Disc. Math.*, Vol. 11, No. 4, 1998, pp. 546-556.

91. (with G. Itkis and S. Rajsbaum) On Mixed Connectivity Certificates, *Theoretical Computer Science*, Vol. 203, 1998, pp. 253-269. [Earlier version in *Algorithms - ESA '95*, P. Spirakis (ed). Lecture Notes in Comp. Sci., Vol. 979, Springer-Verlag 1995, pp. 1-16.]

92. (with A. Avior, T. Calamoneri, A. Litman and A.L. Rosenberg) A Tight Layout of the Butterfly. *Theory of Computing Systems*, Vol. 31, 1998, pp. 475-487.

93. (with A. Biryukov) Cryptanalysis of the Portz Interconnection-Network Block-Cipher. Technical Report #887, Nov. 1996, Technion, Department of Computer Science. 14 pages.

94. (with G. Even) Embedding Interconnection Networks in Grids via the Layered Cross Product. *Networks*, Vol. 36, Issue 2, 2000, pp. 91-95. Also in *Algorithms and Complexity, Third Italian Conference, CIAC'97, Rome, Italy, March 1997, Proceedings*, G. Bongiovanni et.al. (Eds.), Springer, 1997, LNCS Vol. 1203, pp. 3-12.

95. (with E.G. Coffman, Jr.) A Note on Limited Preemption. *Parallel Processing Letters*, Vol. 8, No. 1, 1998, pp. 3-6.

96. Layout Area of Sorting Networks. Feb. 1997. 16 pages. Presented in IWIN'97.

97. (with S. Muthukrishnan, M.S. Paterson and S.C. Sahinalp) Layout of the Batcher Bitonic Sorter. In *SPAA'98 – Tenth Annual ACM Symposium on Parallel Algorithms and Architectures*, pp. 172-181.

98. Four Value-Adding Algorithms, *IEEE Spectrum*, Vol. 35, No. 5, May 1998, pp. 33-38.

99. (with Y. Dinitz, R. Kupershtok and M. Zapolotsky) Some Compact layouts of the Butterfly. In *SPAA'99 – Eleventh Annual ACM Symposium on Parallel Algorithms and Architectures*, pp. 54-63.

100. (with R. Kupershtok) Layout Area of the Hypercube. Manuscript, 22 pages, April 2001.

101. (with S. Bhatt, D. Greenberg and R. Tayar) Traversing Directed Eulerian Mazes. In *Graph Theoretic Concepts in Computer Science*, (Proceedings of WG'2000). U. Brandes and D. Wagner (Eds). Lecture Notes in Computer Science No. 1928, Springer, 2000, pp. 35-46.

## Books

1. *Algorithmic Combinatorics,* Macmillan, January 1973, 260 pages.

2. *Automata, Languages and Programming,* Edited by S. Even and O. Kariv, (Proc. of ICALP 81, Acre, Israel, July 1981) Springer-Verlag Lecture Notes in Computer Science, Vol. 115.

3. *Graph Algorithms,* Computer Science Press, August 1979, 249 pages.

## U.S. Patents

1. (with L.M. Spandorfer and A.B. Tonik) Planar Interconnecting Network Avoiding Signal Path Crossover, April 26, 1966. (Sperry-Rand Corp.) See also 3.407.357, October 22, 1968.

2. Planar Function Generator Using Modulo 2 Unprimed Canonical Form Logic, US Patent 3.291.974, December 13, 1966. (Sperry-Rand Corp.)

3. (with A.J. Lincoln) Fractional Output Frequency Dividing Apparatus, US Patent 3.605.025, September 14, 1971. (Sperry-Rand Corp.)

4. (with S. Micali and O. Goldreich) On-Line/Off-Line Digital Signing, US Patent 5,016,274, May 14, 1991.

5. Systolic Array for Modular Multiplication, US patent 5,101,431, Mar. 31, 1992.

6. Sorting Networks Having Enhanced Layout, US patent 6,021,131, Feb. 1, 2000.

7. Sorting Networks Having Reduced-Area Layouts, US patent application, Serial No. 08/889772, filed July 8, 1997. To be issued.

8. Sorting Networks Having Improved Layouts, US patent application, Serial No. 08/956,061, filed Oct. 22, 1997. To be issued.

9. Switching Networks Having Improved Layouts, US patent 6,018,523, Jan. 25, 2000.

## Graduate Students (partial list)

[M stands for a Master's degree, D stands for a Doctorate degree.]

Igal Golan (M)
Igal Kohavi (M)
Fanica Gavril (D)
Yehoshua Perl (M and D)
Gideon Ehrlich (M and D)
Gavriela Lev (M)
Yossi Shiloach (D)
Alon Itai (M and D)
Oded Kariv (D)
Michael Rodeh (D)
Yacov Yacobi (D)
Reuven Bar-Yehuda (M and D)
Rafi Tayar (M)
Yonathan Stern (M)
Oded Goldreich (M and D)
Baruch Awerbuch (D)
Hillel Gazit (M)
Yair Oren (M)
Yachin Pnueli (M)
Dan Kimmel (M)
Sergio Rajsbaum (D)
Gilad Granot (M)
Aharon Kupershtok (M and D)
Ishai Rabinovitz (M)
Alex Biryukov (D)