Avi Wigderson

Resumé

April 11, 2024

Contents

1 Personal Information

Born: September 9, 1956
Marital Status: Married, three children
Current Address : Institute for Advanced Study, Einstein Drive, Princeton, NJ 08540, USA.

2 Research Interests:

Complexity Theory, Parallel Computation, Combinatorics and Graph Theory, Combinatorial Optimization Algorithms, Randomness and Cryptography, Distributed and Neural Networks.

3 Education

- 1983 — Ph.D in Computer Science, Princeton University, Department of Electrical Engineering and Computer Science.
  Thesis: *Studies in Combinatorial Complexity*
  Advisor: Prof. R.J. Lipton

- 1982 — M.A in Computer Science, Princeton University.

- 1981 — M.S.E in Computer Science, Princeton University.

- 1980 — B.Sc *Summa cum laude* in Computer Science, Technion - Israel Institute of Technology.

4 Honors

- 2024 *A.M. Turing Award*, Association for Computing Machinery

- 2023 *Honorary Doctorate*, The Technion

- 2023 *Edsger W. Dijkstra Prize in Distributed Computing*, ACM Symposium on Principles of Distributed Computing

- 2021 *Abel Prize*, Norwegian Academy of Science and Letters

- 2021 *Member*, Norwegian Academy of Science and Letters

- 2019 *Donald E. Knuth Prize*, Association for Computing Machinery (ACM-SIGACT)

- 2018 *ACM Fellow*, Association for Computing Machinery (ACM-SIGACT)

- 2013 *Member*, National Academy of Sciences

- 2011 *Member*, American Academy of Arts and Sciences

- 2011 *Rothschild Visiting Fellow*, Isaac Newton Institute

- 2010 *Fields Institute Distinguished Lecture Series*

- 2009 *Gödel Prize*, European Association for Theoretical Computer Science and Association for Computing Machinery Special Interest Group on Algorithms and Computation Theory

- 2008 *Conant Prize*, American Mathematical Society

- 2008 *Gibbs Lecture*, American Mathematical Society

- 2006 *International Congress of Mathematicians Plenary Lecture*, Madrid, Spain

- 1994 *The Yoram Ben-Porat Presidential Prize for Outstanding Researcher*

- 1994 *Nevanlinna Prize*, International Mathematical Union

- 1994 *Invited speaker* at the *International Congress of Mathematicians*, Zurich, Switzerland

- 1990 *Invited speaker* at the *International Congress of Mathematicians*, Kyoto, Japan

- 1989 *Bergman Fellowship*

- 1986-89 *Alon Fellowship*

- 1982-83 *IBM Graduate Fellowship*, Princeton University

- 1977-80 *President's List of Excellence*, The Technion

5 Employment

- July, 1999–present *Herbert H. Maass Professor*, School of Mathematics, Institute for Advanced Study, Princeton, NJ.

- 1991–July, 2003 *Professor*, Computer Science Institute, Hebrew University, Jerusalem.

- 1995–1996 *Visiting Professor*, Institute for Advanced Study, Princeton, and Department of Computer Science, Princeton University.

- 1993–95 *Chairman*, Computer Science Institute, Hebrew University, Jerusalem.

- 1990–92 *Visiting Associate Professor*, Department of Computer Science, Princeton University.

- 1987–92 *Associate Professor* (with tenure), Department of Computer Science, Hebrew University, Jerusalem.

- 1986–87 *Senior Lecturer*, Department of Computer Science, Hebrew University, Jerusalem.

- 1985–86 *Fellow*, Mathematical Sciences Research Institute, Berkeley, California.

- 1984–85 *Visiting Scientist*, IBM Research, San Jose, California.

- 1983–84 *Visiting Assistant Professor*, Department of Computer Science, U.C. Berkeley, California.

6 Teaching

- Combinatorics and Graph Theory, Lower Bound Techniques, Data Structures, Algorithms, Probabilistic Algorithms, Circuit Complexity, Introduction to Complexity Theory, Randomness in Computation, The Probabilistic Method, Proof Techniques in Complexity Theory.

7 Postdoc and graduate student supervision

7.1 Post-Docs

- In my CSDM group at the Institute for Advanced Study

- *Anna Gal*, 1995–1996

- *Benjamin Sudakov*, 1999–2003

- *Mikhail Alekhnovitch*, 2000–2001, 2003–2005

- *Nicola Galesi*, 2000–2001

- *Valentine Kabanets*, 2000–2001

- *Satyanarayana Lokam*, 2000–2001

- *Alex Samorodnitsky*, 2000–2001

- *Venkatesh Srinivasan*, 2000–2001

- *Salil Vadhan*, 2000–2001

- *Andris Ambainis*, 2001–2002, 2003–2004

- *Michael Capalbo, 2001–2002*
- *Irit Dinur, 2001–2002*
- *Oded Regev, 2001–2003*
- *Clifford Smyth, 2001–2002*
- *Amit Chakrabarti, 2002–2003*
- *Michael Elkin, 2002–2003*
- *Hartmut Klauck, 2002–2003*
- *Xiaodong Sun, 2002–2003*
- *Boaz Barak, 2003–2005*
- *Maria Chudnovsky, 2003–2005*
- *Subhash Khot, 2003–2004*
- *Ryan O'Donnell, 2003–2004*
- *Nathan Segerlind, 2003-2004*
- *Scott Aaronson, 2004–2005*
- *Eli Berger, 2004–2005*
- *David Galvin, 2004–2005*
- *Guy Kindler, 2004–2005*
- *Dror Weitz, 2004–2005*
- *Andrej Bogdanov, 2005–2006*
- *James Lee, 2005–2006*
- *Eyal Rozenman, 2005–2006*
- *Balasz Szegedy, 2005–2006*
- *Nir Allon, 2006–2007*
- *Julia Chuzhoy, 2006–2007*
- *Nir Halman, 2006–2008*
- *Tali Kaufman, 2006–2008*
- *Neeraj Kayal, 2006–2008*
- *Jonathan Kelner, 2006–2007*
- *Aaron Siegel, 2006–2007*
- *Vladimir Trifonov, 2006–2007*
- *Emanuele Viola, 2006–2007*
- *Adi Akavia, 2007–2009*
- *Xi Chen, 2007–2009*
- *Kevin Costello, 2007–2008*
- *Anup Rao, 2007–2009*
- *Sergey Yekhanin, 2007–2008*

- *Arkadev Chattopadhyay*, 2008–2009

- *Zeev Dvir*, 2008–2011

- *Pavel Hrubes*, 2008–2009

- *Gabor Kun*, 2008–2010

- *Dana Moshkovitz*, 2008–2010

- *Virginia Vassilevska*, 2008–2009

- *Richard Ryan Williams*, 2008–2009

- *Amir Yehudayoff*, 2008–2010

- *Madhur Tulsiani*, 2009–2011

- *Swastik Kopparty*, 2010–2011

- *Shachar Lovett*, 2010–2013

- *Shubhangi Saraf*, 2011–2012

- *Grant Schoenebeck*, 2010–2012

- *Srikanth Srinivasan*, 2010–2012

- *Nikhil Srivastava*, 2010–2012

- *Raghu Meka*, 2011–2013

- *Ankur Moitra*, 2011–2013

- *Jelani Nelson*, 2011–2013

- *Jing Chen*, 2012–2013

- *Andrew Drucker*, 2012–2014

- *Klim Efremenko*, 2012–2013

- *Hao Huang*, 2012–2014

- *Or Meir*, 2012–2014

- *Ali Sinop*, 2013–2014

- *Anindya De*, 2013–2014

- *Edinah Gnang*, 2013–2014

- *Yuval Filmus*, 2013–2015

- *Gillat Kol*, 2013–2016

- *Karim Adiprasito*, 2014–2015

- *Michael Forbes*, 2014–2015

- *Noga Ron-Zewi*, 2014–2015

- *Christopher Beck*, 2014–2016

- *Doron Puder*, 2014–2016

- *Pooya Hatami*, 2015–2016

- *Avishay Tal*, 2015–2017

- *Zeyuan Allen-Zhu*, 2016–2017

- *Aaron Potechin, 2016–2017*

- *Orit Raz, 2016–2017*

- *Eshan Chattopadhyay, 2016–2018*

- *Pravesh Kothari, 2016–2018*

- *Gil Cohen, 2017–2018*

- *Nadav Cohen, 2017–2018*

- *Shay Moran, 2017–2018*

- *Behnam Neyshabur, 2017–2018*

- *Jeroen Zuiddam, 2018–2020*

- *Visu Makam, 2018–2021*

- *Dor Minzer, 2018–2021*

- *Fotis Iliopoulos, 2019–2020*

- *Robert Robere, 2019–2020*

- *Fan Wei, 2019–2020*

- *Vijay Bhattiprolu, 2020–2022*

- *Lisa Sauermann, 2020–2021*

- *Lior Alon, 2020–2022*

- *Matija Bucic, 2021–2023*

- *Or Zamir, 2021–2023*

- *Leonardo Coregliano, 2021–2023*

- *Fernando Granha Jeronimo, 2021–2023*

- *Roei Tell, 2021–2023*

- *Pei Wu, 2021–2023*

- At the Hebrew University

  - *Mario Szegedy, 1989–1990*
  - *David Zuckerman, 1993–1994*
  - *Jiri Sgall, 1994–1995*
  - *Jaikumar Radhakrishnan, 1996–1997*
  - *Shiyu Zhou, 1996–1997*

7.2 Graduate student Supervision

- Ph.D

  - *Prabhakar Ragde*, U. C. Berkeley, co-advisor with *R. Karp*, 1983–1986.
    Ph.D Thesis: *Lower bounds for parallel computation*

  - *Mauricio Karchmer*, Hebrew University, 1986–1988.
    Ph.D Thesis: *Complexity of computation and restricted machines*,
    Winner of the *ACM Best Doctoral Thesis in Computer Science Award*.

  - *Moti Reif*, Ben-Gurion University, co-advisor with *M. Rubin*, 1987–1988.
    Ph.D Thesis: *Parallel algorithms for convex sets in R^2 and R^3*.

- *Joseph Gil*, Hebrew University, 1986–1990.
  Ph.D. Thesis: *Lower bounds and algorithms for hashing and parallel processing.*

- *Aviad Cohen*, Hebrew University, 1986–1991.
  Ph.D. Thesis: *Disperser graphs, deterministic amplification and imperfect random sources.*

- *Ilan Newman*, Hebrew University, 1987–1991.
  Ph.D. Thesis: *On the formula complexity of simple boolean functions.*

- *Rafi Heyman*, Weizmann Institute, co-advisor with *D. Harel*, 1987–1991.
  Ph.D. Thesis: *Randomized decision tree complexity of read-once Boolean functions.*

- *Ran Raz*, Hebrew University, co-advisor with *M. Ben-Or*, 1988–1992.
  Ph.D. Thesis: *Communication complexity and circuit lower bounds.*

- *Yuri Rabinovich*, Hebrew University, co-advisor with *N. Linial*, 1988–1992.
  Ph.D. Thesis: *Monlinear Mixing and evolution of Combinatorial Systems.*

- *Roy Armoni*, Hebrew University, co-advisor with *M. Ben-Or*, 1994–1998.
  Ph.D. Thesis: *On the Random Resources Needed by Space-Bounded Computational Models.*

- *Dorit Aharonov*, Hebrew University, co-advisor with *M. Ben-Or*, 1994–1998.
  Ph.D. Thesis: *Noisy Quantum Computation.*

- *Ronen Shaltiel*, Hebrew University, 1997–2001.
  Ph.D. Thesis: *Explicit Constructions of Pseudo-Random Generators and Extractors.*

- *Amir Shpilka*, Hebrew University, 1997–2001.
  Ph.D. Thesis: *Lower Bounds for Small Depth Arithmetic and Boolean Circuits.*

- *Eli Ben-Sasson*, Hebrew University, 1997–2001.
  Ph.D. Thesis: *Expansion in Proof Complexity.*

- *David Xiao*, Princeton University, co-advisor with Boaz Barak, 2004–2009.
  Ph.D. Thesis: *New Perspectives on the Complexity of Computational Learning, and Other Problems in Theoretical Computer Science.*

- M.Sc Students

  - *Ron Ben-Nathan*, Hebrew University, 1987–1990.
    MSc Thesis: *Transforming Probabalistic to Deterministic Algorithms.*

  - *Shlomo Huri*, Hebrew University, 1987–1990.
    MSc Thesis: *Universal sequences for expander graphs and contracting sequences on graphs.*

  - *Michal Parnas*, Hebrew University, 1987–1990.
    MSc Thesis: *Approximate Counting, Almost Uniform Generation and Random Walks.*

  - *Roded Sharan*, Hebrew University, 1994–1995.
    MSc Thesis: *Perfect Matching in Parallel Computation.*

  - *Dana Pe'er*, Hebrew University, 1997–1999.
    MSc Thesis: *On Minimum Spanning Trees.*

  - *Ziv Bar-Yossef*, Hebrew University, 1997–1998.
    MSc Thesis: *Deterministic Amplification of Space-Bounded Randomized Algorithms.*

8   Personal Grants

- U.S. National Science Foundation, *Theory of Computation - New Algorithmic and Hardness Techniques*, 2019–2023.

- U.S. National Science Foundation, *Theory of Computation - Pushing the State-of-the-Art* (with *Ran Raz*), 2014–2019.

- U.S. National Science Foundation, *Computational Complexity Theory* (with *Alexander Razborov*), 2009–2014.

- U.S. National Science Foundation, *Expeditions in Computing, or Understanding, Coping with, and Benefiting from, Intractability* (with *Russell Impagliazzo, Princeton University*), 2008–2013.

- U.S. National Science Foundation, *Pseudorandomness* (with *Russell Impagliazzo, Peter Sarnak and Jean Bourgain*), 2008–2012.

- U.S. National Science Foundation, *Lie Groups, Representations and Discrete Mathematics* (with *Alexander Lubotzky*), 2007–2008.

- U.S. National Science Foundation, *Basic Research in Theoretical Computer Science and Discrete Mathematics* , 2000–2003.

- U.S. National Science Foundation, *Special Year in Computational Complexity Theory* , 2000–2001.

- Israeli National Science Foundation, *Algebraic and Combinatorial Computation: Models, Methods and Connections* (with *M. Ben-Or and N. Nisan, Hebrew University*), 1996–1999.

- US-Israel Binational Science Foundation, *Inherent Complexity of Computational Problems* (with *A. Yao, Princeton University* and *M. Karchmer, MIT*), 1993–1996.

- Wolfson Foundation *Randomness in Computation* (with *N. Nisan, Hebrew University*, 1993–1996

- Wolfson Foundation *Randomness in Computation* (with *N. Nisan, Hebrew University*, 1990-1993.

- US-Israel Binational Science Foundation, *Inherent Complexity of Computational Problems* (with *M. Sipser, MIT* and *M. Ben-Or, Hebrew University*), 1988–1990.

- U.S. National Science Foundation, *Research on the Relative Power of Randomizing and Deterministic Algorithms* (with *R.M. Karp, U.C. Berkeley*), 1987–1988.

- Israeli National Academy of Sciences, *Implementing Probabilistic Algorithms* (with *M. Ben-Or, Hebrew University*), 1987–1988.

- Alon Fellowship, Hebrew University 1986–1989.

9   Some Invited Talks

- Bowen lectures at University of California, Berkeley, Berkeley, USA, 2018.

- AMS Colloquium Lectures at the Joint Mathematics Meetings, San Diego, USA, 2018.

- STOC 2017 Plenary Lecture, 49th Annual ACM Symposium on the Theory of Computing, Montreal, Canada, 2017.

- ETH Turing Center Opening Lectures at ETH Zurich, Zurich, Switzerland, 2016.

- The Ada Lovelace Bicentenary Lectures on Computability at IIAS, Jerusalem, Israel, 2016.

- Indira Foundation Distinguished Lectures at IIT Bombay, Mumbai, India, 2015.

- Ahlfors Lecture at Harvard University, Cambridge, USA, 2014.

- Green Family Lecture Series at IPAM, Los Angeles, USA, 2014.

- Leonidas Alaoglu Memorial Lecture at Caltech, Los Angeles, USA, 2014.

- Heidelberg Laureate Forum, Heidelberg, Germany, 2013.

- The 10th annual conference on Theory and Applications of Models of Computation, Hong Kong, China, 2013.

- Center for Quantum Technologies 5th Anniversary Symposium, Singapore, 2012.

- Wolfgang Pauli Lectures, Zürich, Switzerland, 2012

- International Congress on Mathematical Physics, Aalborg, Denmark, 2012.

- International Center for Theoretical Sciences Inaugural Event, Bangalore, India, 2009.

- International Congress of Mathematicians, Madrid, Spain, 2006.

- Fields Insitute Distinguished Lecture Series, Ontario, Canada, 1998.

- International Congress of Mathematitians, Zurich, Switzerland, 1994.

- International Federation for Information Processing, Hamburg, Germany 1994.

- International Colloquium on Automata, Languages and Programming, Jerusalem, Israel, 1994.

- Symposium on the Theory of Computing, Montreal, Canada, 1994.

- Mathematical Foundations of Computer Science, Prague, Czechoslovakia, 1992.

- International Congress of Mathematitians, Kyoto, Japan 1990.

10 Editorship

- *Journal of the Association for Computing Machinery*, Associate Editor.

- *Journal of the American Mathematical Society*, Associate Editor.

- *SIAM Journal on Discrete Mathematics*, Editorial Board.

- *Information and Computation*, Editorial Board.

- *Complexity Theory*, Editorial Board.

11 Scientific Boards

- *Simons Foundation*, Scientific Advisory Board.

- *Simons Institute for the Theory of Computing*, Scientific Advisory Board.

12 Program Committees of International Conferences

- *Program Committee Chair:* STOC '92.

- *Program Committee Member:* STOC '12, ISTCS '94, ICALP '90, STOC '89, STRUCTURES '89, STOC '86.

13 Referee

- Book Reviews: *Addison Wesley.*

- Fellowships: *The Royal Society.*

- Grant Proposals: *Israel Academy of Sciences, U.S. National Science Foundation, National Sciences and Engineering Council of Canada, American-Israeli Binational Science Foundation.*

- Scientific Journals: *Journal of the ACM, SIAM Journal on Computing, Theoretical Computer Science, Journal of Algorithms, IEEE Transactions on Information Theory, Journal of Computer Systems and Sciences, Information Processing Letters, Information and Control, Science of Computer Programming, Acta Informatica, Algorithmica, Advances in Computing Research, Journal of Complexity, Combinatorica, Journal of Economic Theory.*

14 References

- Professor Richard M. Karp, U.C. Berkeley.

- Professor Alan Borodin, University of Toronto.

- Professor Andy Yao, Tsinghua University.

- Professor Richard Lipton, Georgia Tech.

- Professor Lazlo Lovasz, Eötvös Loránd University.

- Professor Lesley Valiant, Harvard University.

- Professor Michael Rabin, Columbia University.

- Professor Nicholas Pippenger, Harvey Mudd College.

15 Scientific Publication

Ph.D Thesis: *Studies in Computational Complexity*, Princeton University, June 1983.
Advisor: Professor R.J. Lipton.

15.1 Scientific Journals:

1. A. Wigderson, *Improving the Performance for Approximate Graph Coloring*, Journal of the ACM, Vol. 30, No. 4, pp. 729–735, October 1983.

2. G. Vijayan, A. Wigderson, *Rectilinear Graphs and their Embedding*, SIAM Journal on Computing, Vol. 14, No. 2, pp. 355–372, May 1985.

3. U. Vishkin, A. Wigderson, *Depth-Width Trade-offs in Parallel Processing*, SIAM Journal on Computing, Vol. 14, No. 2, pp. 303–314, May 1985.

4. H. Galperin, A. Wigderson, *Succinct Representation of Graphs* , Information and Control, Vol. 56, No. 3, pp. 183–198, March 1984.

5. U. Vishkin, A. Wigderson, *Dynamic Parallel Memories*, Information and Control, Vol. 56, No. 3, pp. 174–182, March 1984.

6. R. Karp, A. Wigderson, *A Fast Parallel Algorithm for the Maximal Independent Set Problem*, Journal of the ACM, Vol. 32, No. 4, pp.762–773, October 1985.

7. R. Karp, E. Upfal, A. Wigderson, *Constructing a Perfect Matching is in Random NC*, Combinatorica, Vol. 6, No. 1, pp. 35–48, 1986.

8. M. Perry, A. Wigderson, *Search in a Known Pattern*, Journal of Political Economy, Vol. 94, No. 1, pp. 225–230, 1986.

9. A. Borodin, F.E. Fich, F. Meyer auf der Heide, E. Upfal, A. Wigderson, *A Time-Space Tradeoff for Element Distinctness*, SIAM Journal on Computing, Vol. 16, No. 1, pp. 97–99, February 1987.

10. E. Upfal, A. Wigderson, *How to Share Memory in a Distributed System*, Journal of the ACM, Vol. 34, No. 1, pp.116–127, 1986.

11. D. Long, A. Wigderson, *The Discrete Logarithm Hides O(log n) Bits*, SIAM Journal on Computing, Vol. 17, No. 2, pp. 363–372, 1988.

12. F. Meyer auf der Heide, A. Wigderson, *The Complexity of Parallel Sorting*, SIAM Journal on Computing, Vol. 16, No. 1, pp. 100–107, 1987.

13. F. Fich, F. Meyer auf der Heide, A. Wigderson, *Lower Bounds for Parallel Random Access Machines with Unbounded Shared Memory*, Advances in Computing Research - Parallel and Distributed Computing, Ed. F. Preparata, Vol. 4, pp 1-16, 1987.

14. F. Fich, P. Ragde, A. Wigderson, *Simulations among Concurrent-Write PRAMs*, Algorithmica, Vol. 3, pp. 43–51, 1988.

15. M. Ajtai, A. Wigderson, *Deterministic Simulation of Probabilistic Constant-Depth Circuits*, Advances in Computing Research - Randomness and Computation, Ed. F. Preparata and S. Micali, Vol. 5, pp. 199-223, 1989

16. Faith E. Fich, P. Ragde, A. Wigderson, *Relations between Concurrent-Write Models of Parallel Computation* , SIAM Journal on Computing, Vol. 17, No. 3, pp. 606–627, 1988.

17. A. Borodin, F.E. Fich, F. Meyer auf der Heide, E. Upfal, A. Wigderson, *A tradeoff between Search and Update Time for the Implicit Dictionary Problem*, Theoretical Computer Science, Vol. 58, pp. 57–68, 1988.

18. Richard M. Karp, E. Upfal and A. Wigderson, *The Complexity of Parallel Search*, Journal of Computer and System Sciences, Vol. 36, No. 2, pp. 225–253, 1988.

19. N. Linial, L. Lovasz and A. Wigderson, *Rubber Bands, Convex Embeddings and Graph Connectivity*, Combinatorica, Vol. 8, pp.91–102, 1988.

20. P. Ragde, W. Steiger, E. Szemeredi and A. Wigderson, *The Parallel Complexity of Element Distinctness is* $\Omega(\sqrt{\log n})$, SIAM Journal on Discrete Mathematics, Vol. 1, No. 3, pp. 399–410, 1988.

21. M. Karchmer, N. Linial, I. Newman, M. Saks and A. Wigderson, *Combinatorial Characterization of Read-Once Formulæ*, J. Discrete Math. Vol. 114, pp. 275–282, 1993.

22. O. Goldreich, S. Micali and Avi Wigderson, *Proofs that Yield Nothing but their Validity, or All Languages in NP have Zero-Knowledge Proof Systems*, Journal of the ACM, Vol. 38, No. 1, pp. 691–729, 1991.

23. N. Alon, M. Karchmer and A. Wigderson, *Linear Circuits over* $GF(2)$, SIAM Journal on Computing, Vol. 19, No. 6, pp. 1064-1067, 1990.

24. F. Fich and A. Wigderson, *Towards Understanding Exclusive Reads*, SIAM Journal on Computing, Vol. 19, No. 4, pp. 718–727, 1990.

25. M. Karchmer and A. Wigderson, *Monotone Circuits for Connectivity require Super-Logarithmic Depth*, SIAM Journal on Discrete Mathematics, Vol. 3, No. 2, pp. 255-265, 1990.

26. P. Ragde and A. Wigderson, *Linear–Size Constant–Depth Polylog– Threshold Circuits* , Information Processing Letters, Vol. 39, No. 3, pp. 143-146, 1991.

27. N. Nisan and A. Wigderson, *Rounds in Communication Complexity Revisited*, SIAM Journal on Computing, Vol. 22, No. 1, pp. 211–219, 1993.

28. R. Heiman, I. Newman and A. Wigderson, *On Read–Once Threshold Formulae and their Randomized Decision Tree Complexity*, Theoretical Computer Science, Vol. 107, No. 1, pp. 63–76, 1990.

29. Y. Gil, W. Steiger and A. Wigderson, *Geometric Medians*, Discrete Math, Vol. 108, No. 1, pp. 37–51, 1992.

30. L. Babai, L. Fortnow, N. Nisan and A. Wigderson, *BPP has Subexponential Time Simulations unless EXPTIME has Publishable Proofs*, Complexity Theory, Vol. 3, pp. 307–318, 1993.

31. R. Heiman and A. Wigderson, *Randomized vs. Deterministic Decision Tree Complexity for Read–Once Boolean Functions*, Complexity Theory, Vol. 1, pp. 311–329, 1991.

32. R. Raz, A. Wigderson, *Monotone Circuits for Matching require Linear Depth*, Journal of the ACM, Vol. 39, pp. 736-744, 1992.

33. N. Nisan, A. Wigderson, *Hardness vs. Randomness*, Journal of Computer Systems and Sciences, Vol. 49, No. 2, pp. 149–167, 1994.

34. I. Newman, A. Wigderson, *Lower Bounds on Formula Size of Boolean Functions using Hypergraph Entropy*, SIAM Journal on Discrete Mathematics, Vol. 8 No. 4, pp. 78–87, 1996.

35. J. Friedman and A. Wigderson, *On the Second Largest Eigenvalue of Hypergraphs*, Combinatorica, Vol. 15, No. 1, pp. 43–65, 1995.

36. J. Hastad and A. Wigderson, *Composition of the Universal Relation*, in "Advances in Computational Complexity Theory", AMS-DIMACS book series in Discrete Mathematics and Theoretical Computer Science, Vol. 13, pp. 119–134, 1993.

37. S. Ben-David, A. Borodin, R. Karp, G. Tardos, A. Wigderson, *On the Power of Randomization in On-line Algorithms*, Algorithmica, Vol. 11, No. 1, pp. 2–14, 1994.

38. B. Yust, M. Meyer auf der Heide, A. Wigderson, *On Computations with Integer Division*, Theoretical Informatics and Applications, Vol. 23, No. 1, pp. 101–111, 1989.

39. S. Hoory and A. Wigderson, *Universal Sequences for Expander Graphs*, Information Processing Letters, Vol. 46, No. 2, pp. 67–69, 1993.

40. A. Razborov, E. Szemeredi, A. Wigderson, *Constructing Small Sets that are Uniform in Arithmetic Progressions*, Probability, Combinatorics and Complexity, Vol. 2, pp. 513–518, 1993.

41. A. Razborov and A. Wigderson, $n^{\Omega(\log n)}$ *Lower Bounds on the Size of Depth 3 Threshold Circuits with AND Gates at the Bottom*, IPL, Vol. 45, pp. 303–307, 1993.

42. M. Karchmer, I. Newman, M. Saks, A. Wigderson, *Non– deterministic Communication Complexity with Few Witnesses*, JCSS, Vol. 49, No. 2, 1994.

43. N. Alon, U. Feige, A. Wigderson, D. Zuckerman, *Derandomized Graph Products*, Computational Complexity, pp. 60-75, 1995.

44. Y. Gil, F. Meyer auf der Heide, A. Wigderson, *The Tree Model for Hashing: Lower and Upper Bounds*, SIAM J. on Computing, Vol. 10, pp. 936–955, 1996.

45. H. Alt, L. Guibas, R. Karp, K. Mehlhorn and A. Wigderson, *A Method for Obtaining Probabilistic Algorithms with Small Tail Probabilities*, Algorithmica, Vol. 16, No. 4-5, pp. 543–547, 1996.

46. A. Condon, L. Hellerstein, S. Pottle, A. Wigderson, *Finite State Automata with Nondeterministic and Probabilistic States*, SIAM J. on Computing, Vol. 27, No. 3, pp. 739-762, June 1998.

47. L. Lovasz, I. Newman, M. Naor, A. Wigdreson, *Search Problems in the Decision Tree Model*, SIAM J. on Discrete Math., Vol. 8, pp. 119–132, 1995.

48. N. Nisan, A. Wigderson, *A note on Rank vs. Communication Complexity*, Combinatorica, Vol. 15, No 4, pp. 557–566, 1995.

49. A. Gál, A. Wigderson, *Boolean Complexity Classes vs. Their Arithmetic Analogs*, Random Structures and Algorithms, Vol. 9, pp. 1–13, 1996.

50. M. Karchmer, R. Raz and A. Wigderson, *Super–Logarithmic Depth Lower Bounds via Direct Sum in Communication Complexity*, Computational Complexity, Vol. 5, pp. 191–204, 1995.

51. P. Miltersen, N. Nisan, S. Safra, A. Wigderson, *On Data Structures and Asymmetric Communication Complexity*, JCSS, Vol. 57, No. 1, pp. 37–49, 1998.

52. A. Gal and A. Wigderson, *Boolean complexity classes vs. their arithmetic analogs*, Random Structures and Algorithms, Vol. 9, Nos. 1 and 2, pp. 99-111, 1996.

53. O. Goldreich, A. Wigderson, *Tiny Families of Functions with Random Properties: A Quality–Size Trade–off*, Random Structures and Algorithms, Vol. 11, No. 4, pp. 315–343, 1997.

54. R. Armoni, A. Ta-Shma, A. Wigderson, S. Zhou, *An $0(\log(n)\frac{4}{3})$ space algorithm for (s,t) connectivity in undirected graphs*, J. ACM Vol. 47, No. 2, 294–311, 2000.

55. L. Babai, A. Gál, A. Wigderson, *Superpolynomial lower bounds for monotone span programs.*, Combinatorica Vol. 19, No. 3, 301–319, 1999.

56. A. Wigderson, D. Zuckerman, *Expanders that beat the eigenvalue bound: explicit construction and applications.* Combinatorica Vol. 19, No. 1, 125–138, 1999.

57. Y. Rabinovich, A. Wigderson, *Techniques for bounding the convergence rate of genetic algorithms.* Random Structures Algorithms Vol. 14, No. 2, 111–138, 1999.

58. O. Reingold, S. Vadhan, A. Wigderson *Entropy Waves, the Zig-Zag Graph Product, and New Constant-Degree Expanders*, Annals of Math, Vol 155, No 1 157–187, 2002.

59. A. Shpilka, A. Wigderson *Depth-3 Arithmetic Formulae over Fields of Characteristic Zero*, Journal of Computational Complexity, Vol 10, No 1, 1–27, 2001.

60. E. Ben-Sasson, A. Wigderson *Space Complexity in Propositional Calculus*, SIAM Journal of Computing, 31 No 4, 1184–1211, 2001.

61. A. Wigderson *On the Work of Madhu Sudan*, Notices of the AMS, 50, No 1, 45–50, 2003.

62. J. Hastad, A. Wigderson *Simple Analysis of Graph Tests for Linearity and PCP*, Random Structures and Algorithms, Vol 22, No 2, 139–160, 2003.

63. R. Impagliazzo, V. Kabanets, A. Wigderson *In Search of an Easy Witness: Exponential Time vs. Probabilistic Polynomial Time*, JCSS, Vol. 65, No. 4, 672–694, 2002.

64. E. Ben-Sasson, R. Impagliazzo, A. Wigderson *Near Optimal Separation of Tree-Like and General Resolution*, Combinatorica, Vol. 24, Issue 4, 585–604, 2003.

65. A. Ambainis, L. Schulman, A. Ta-Shma, Vazirani, A. Wigderson, *The Quantum Communication Complexity Sampling*, Siam Journal on Computing, Vol 32, No 6, 1570–1585, 2003.

66. A. Razborov, A. Wigderson, A. Yao, *Read-once Branching Programs, Rectangular Proofs of the Pigeonhole Principle and the Transversal Calculus*, Combinatorica, Vol 22, No 4, 555–574, 2003.

67. R. Meshulam, A. Wigderson *Expanders in Group Algebras*, Combinatorica, Vol. 24, Issue 4, 659–680, 2004.

68. M. Alekhnovitch, E. Ben-Sasson, A. Razborov, A. Wigderson, *Pseudorandom Generators in Propositional Proof Complexity*, SIAM Journal on Computing, Vol 34, Number 1, 2004.

69. E. Ben Sasson, R. Impagliazzo, A. Wigderson, *Near Optimal Separation of Tree-like and General Resolution*, Combinatorica, Vol 24, Issue 4, pp 585–604, 2004.

70. B. Barak, R. Impagliazzo, A. Wigderson, *Extracting randomness using few independent sources*, SICOMP, Vol 36, Number 3, 2006.

71. A. Shpilka, A. Wigderson, *Derandomizing homomorphism testing in general groups*, SICOMP, Vol 36, Number 3, 2006.

72. O. Reingold, R. Shaltiel, A. Wigderson, *Extracting Randomness via Repeated Condensing*, SIAM Journal on Computing, Vol 35, Number 5, pp. 1185–1209, 2006.

73. P. Beame, T. Pitassi, N. Segerlind, A. Wigderson, *A Strong Direct Product Theorem for Corruption and the Multiparty NOF Communication Complexity of Set Disjointness*, Special Issue Computational Complexity, 2006.

74. E. Rozenman, A. Shalev, A. Wigderson, *Iterative Construction of Cayley Expander Graphs*, Theory of Computing, 2/5, pp 91–120, 2006.

75. R. Impagliazzo, R. Shaltiel, A. Wigderson, *Reducing the seed length in the Nissan-Wigderson generator*, Combinatorica, 26 (6), pp. 647–681, 2006.

76. A. Wigderson, D. Xiao, *Derandomizing the AW matrix-valued Chernoff bound using pessimistic estimators and applications*, Electronic Colloquium on Computational Complexity, Report TR06-105, ISSN 1433–8092, 13th Year, 105th Report.

77. S. Hoory, N. Linial, A. Wigderson, *Expander graphs and their applications*, Bulletin of the American Mathematical Society, Vol. 43, No. 4, pp 439–561, 2006.

78. E. Rozenman, A. Shalev, A. Wigderosn, *Iteartive construction of Cayley expander graphs*, Theory of Computing, Vol. 2, No. 5, pp. 91-120, 2006. A Shorter version appeared in STOC 04.

79. A. Wigderson, D. Xiao, *Derandomizing the AW matric-valued Chernoff bound using pessimistic estimators and applications*, Theory of Computing, Vol. 4, article 3, pp. 53-76, 2008.

80. G. Kalai, A. Wigderson, *Neighborly Embedded Manifolds*, Discrete and Computational Geometry, Vol. 40, No. 3., October 2008.

81. E. Viola, A. Wigderson, *Norms, XOR lemmas, and lower bounds for polynomials and protocols*, Theory of Computing, Vol. 4, Article 7, pp. 137-168, 2008.

82. Z. Dvir, A. Gabizon, A. Wigderson, *Extractors and rank extractors for polynomial sources*, Computational Complexity, Vol. 18, No. 1, pp. 1-58, 2009.

83. R. Impagliazzo, R. Jaiswal, V. Kabanets, A. Wigderson, *Uniform direct product theorems: Simplified, optimized, and derandomized*, SIAM Journal on Computing, Vol. 39, No. 4, pp. 1637-1665, 2010.

84. B. Barak, G. Kindler, R. Shaltiel, B. Sudakov, A. Wigderson, *Simulating independence: New constructions of condensers, ramsey graphs, dispersers, and extractors*, Journal of the ACM, Vol. 57, No. 4, pp. 20:1-20:52, 2010.

85. O. Goldreich, S. Vadhan, A. Wigderson, *Simplified derandomization of BPP using a hitting set generator*, Studies in Complexity and Cryptography, Vol. 6650, pp. 56-67, 2011.

86. Z. Dvir, A. Wigderson, *Kakeya sets, new mergers, and old extractors*, SIAM Journal on Computing, Vol. 40, No. 3, pp. 778-792, 2011.

87. X. Chen, N. Kayal, A. Wigderson, *Partial derivatives in arithmetic complexity and beyond*, Foundations and Trends in Theoretical Computer Science, Vol. 6, No. 1-2, pp. 1-138, 2011.

88. R. Impagliazzo, V. Kabanets, A. Wigderson, *New direct-product testers and 2-query PCPs*, SIAM Journal on Computing, Vol. 41, No. 6, pp. 1722-1768, 2012.

89. G. Kindler, A. Rao, R. O'Donnell, A. Wigderson, *Spherical cubes: Optimal foams from computational hardness amplification*, Communications of the ACM, Vol. 55, No. 10, pp. 90-97, 2012.

90. P. Hrubeš, A. Wigderson, A. Yehudayoff, *An asymptotic bound on the composition number of integer sums of squares formulas*, Canadian Mathematical Society, Vol. 56, No. 1, pp. 70-79, 2013.

91. P. Hrubeš, A. Wigderson, *Non-commutative arithmetic circuits with division*, Theory of Computing, Vol. 11, pp. 357-393, 2014.

92. A. Ai, Z. Dvir, S. Saraf, A. Wigderson, *Sylvester-gallai Type Theorems for Approximate Collinearity*, Forum of Mathematics, Sigma, Vol. 2, 2014.

93. Z. Dvir, S. Saraf, A. Wigderson, *Improved rank bounds for design matrices and a new proof of Kelly's theorem*, Forum of Mathematics, Sigma 4, Vol. 2, 2014.

94. E. Abbe, A. Shpilka, A. Wigderson, *Reed-Muller codes for random erasures and errors*, IEEE Transactions on Information Theory, Vol. 61, No. 10, pp. 5229-5252, 2015.

95. P. Gopalan, R. Servedio, A. Tal, A. Wigderson, *Degree and Sensitivity: tails of two distributions*, ECCC Report TR16-069, pp. 1-31, 2016.

96. A. Wigderson, A. Yehudayoff, *Population Recovery and Partial Identification*, Journal of Machine Learning, Vol. 102, No. 1, pp. 29-56, 2016.

97. T. Kaufman, A. Wigderson, *Symmetric LDPC codes and local testing*, Combinatorica, Vol. 36, No. 1, pp. 92-120, 2016.

98. P. Gopalan, R. Servedio, A. Tal, A. Wigderson, *Degree and Sensitivity: tails of two distributions*, ECCC, Report TR16-069, pp. 1-31, 2016.

99. E. Viola, A. Wigderson, *Local Expanders*, Springer, Computational Complexity, DOI 10.1007/s00037-017-0155-1, 2017.

100. Z. Dvir, S. Saraf, A. Wigderson, *Superquadratic Lower Bound for 3-Query Locally Correctable Codes over the Reals*, Theory of Computing, Vol. 13, No. 11, pp. 1-36, 2017.

101. O. Meir, A. Wigderson, *Prediction from Partial Information and Hindsight, with Application to Circuit Lower Bounds*, ECCC, Report TR17-149, pp. 1-22, 2017.

102. D. Gavinsky, O. Meir, O. Weinstein, A. Wigderson, *Toward Better Formula Lower Bounds: the Composition of a Function and a Universal Relation*, SIAM Journal on Computing (SICOMP), Vol. 46, No. 1, pp. 114-131, 2017.

103. A. Garg, L. Gurvits, R. Oliveira, A. Wigderson, *Algorithmic and optimization aspects of Brascamp-Lieb inequalities, via Operator Scaling*, Geometric and Functional Analysis 2018, https://doi.org/10.1007/s00039-018-0434-2

104. S. Moran, A. Shpilka, A. Wigderson, A. Yehudayoff, *Teaching and compressing for low VC-dimension*, to appear in Journey Through Discrete Mathematics. A Tribute to Jiri Matousek.

15.2 Refereed Conferences

Note: Full versions of the papers numbered 1, 4–14, 18–20, 22, 24, 27–29, 32, 34–36, 38–40, 53, appeared in journals.

1. A. Wigderson, *A New Approximate Graph Coloring Algorithm*, Proc. of the 14th STOC, pp. 325–329, May 1982.

2. D. Dolev, C. Dwork, N. Pippenger, A. Wigderson, *Superconcentrators, Generalizers, and Generalized Connectors with Limited Depth*, Proc. of the 15th STOC, pp. 42–51, May 1983.

3. D. Dolev, A. Wigderson, *The Security of Multi-Party Protocols in Distributed Systems*, Proc. of the Crypto 82 Conference, pp. 167–176, August 1982.

4. D. Long, A. Wigderson, *How Discreet is the Discrete Log?*, Proc. of the 15th STOC, pp. 413–420, May 1983.

5. U. Vishkin, A. Wigderson, *Depth-Width Trade-offs in Parallel Computation*, Proc. of the 24th FOCS, pp. 146–153, November 1983.

6. R. Karp, A. Wigderson, *A Fast Parallel Algorithm for the Maximal Independent Set Problem*, Proc. of the 16th STOC, pp. 266–272, May 1984.

7. F. Fich, P.Ragde, A. Wigderson, *Relations Between Concurrent-Write Models of Parallel Computation*, Conference on the Principles of Distributed Computation, August 1984.

8. E. Upfal, A. Wigderson, *How to Share Memory in a Distributed System*, Proc. of the 25th FOCS, pp. 171–180, October 1984.

9. R. Karp, E. Upfal, A. Wigderson, *Constructing a Perfect matching is in Random NC*, Proc. of the 17th STOC, pp. 22–32, May 1985.

10. F. Fich, F. Meyer auf der Heide, P. Ragde, A. Wigderson, *One, Two, Three...Infinity: Lower Bounds for Parallel Computation*, Proc of the 17th STOC, pp. 48–58, May 1985.

11. R. Karp, E. Upfal, A. Wigderson, *Are Search and Decision Problems Computationally Equivalent?* Proc. of the 17th STOC, pp. 464–475 May 1985.

12. M. Ajtai, A. Wigderson, *Deterministic Simulation of Probabilistic Constant- Depth Circuits*, Proc. of the 26th FOCS, pp. 11–19, October 1985.

13. F. Meyer auf der Heide, A. Wigderson, *The Complexity of Parallel Sorting*, Proc. of the 26th FOCS, pp. 532–540, October 1985.

14. R. Karp, E. Upfal, A. Wigderson, *The Complexity of Parallel Computation on Matroids*, Proc. of the 26th FOCS, pp. 541–550, October 1985.

15. A. Aggarawal, M. Klawe, D. Lichtenstein, N. Linial, A. Wigderson, *Multilayer Grid Embedding*, Proc of the 26th FOCS, pp. 186–196, October 1985.

16. M. Saks, A. Wigderson, *Probabilistic Boolean Decision Trees and the Complexity of Evaluating Game Trees*, Proc. of the 27th FOCS, pp. 29–38, October 1986.

17. R. Karp, M. Saks, A. Wigderson, *A Search Problem Related to Branch-and-Bound Procedures*, Proc. of the 27th FOCS, pp. 19–28, October, 1986.

18. N. Linial, L. Lovasz and A. Wigderson, *A Physical interpretation of graph connectivity and its algorithmic applications*, Proc of the 27 FOCS, pp.39–48, October 1986.

19. O. Goldreich, S. Micali, A. Wigderson, *Proofs that Yield Nothing but their Validity, and a Methodology of Cryptographic Protocol Design*, Proc. of the 27th FOCS, pp. 174–187, October 1986.

20. A. Borodin, F.E. Fich, F. Meyer auf der Heide, E. Upfal, A. Wigderson, *A Tradeoff Between Search and Update Time for the Implicit Dictionary Problem*, Proc. of the 13th ICALP Conference, July, 1986.

21. N. Megiddo, A. Wigderson, *On Play by Means of Computing Machines* Conference on Theoretical Aspects of Reasoning about Knowledge, pp. 259–274, March 1986.

22. A. Borodin, F.E. Fich, F. Meyer auf der Heide, E. Upfal, A. Wigderson, *A Time-Space Tradeoff for Element Distinctness*, Proc. of STACS Conference, pp. 29–37, 1988.

23. O. Goldreich, S. Micali, A. Wigderson, *How to Play any Mental Game*, Proc. of the 19th STOC, pp. 218–229, May 1987.

24. M. Karchmer, A. Wigderson, *Monotone Connectivity Circuits require Super-logarithmic Depth*, Proc. of the 20th STOC, pp. 539–550, May 1988.

25. S. Goldwasser, M. Ben-Or, A. Wigderson, *Completeness Theorems for Non-cryptographic Fault-tolerant Distributed Computing*, Proc. of the 20th STOC, pp. 1–10 May 1988.

26. S. Goldwasser, J. Kilian, M. Ben-Or, A. Wigderson, *Multi- Prover Interactive Proofs: How to Remove Intractability Assumptions* Proc. of the 20th STOC, pp. 113-131, May 1988.

27. F. E. Fich, A. Wigderson, *Towards Understanding Exclusive Read*, Proc. of 1st Symposium on Parallel Algorithms and Architectures, pp. 718–727, August 1990.

28. B. Yust, F. Meyer auf der Heide, A. Wigderson, *On Computations with Integer Division*, Proc. of the STACS conference, pp. 29–37, 1988.

29. N. Nisan, A. Wigderson, *Hardness vs. Randomness*, Proc. of the 29th FOCS, pp. 2–11, 1988.

30. R. Raz, A. Wigderson, *Probabilistic Communication Complexity of Boolean Relations*, Proc of the 30th FOCS, pp. 562–567, 1989.

31. A. Cohen, A. Wigderson, *Dispersers, Deterministic Amplification and Weak random Sources*, Proc. of the 30th FOCS, pp. 14–19, 1989.

32. M. Ben-Or, S. Goldwasser, J. Kilian and A. Wigderson, *Efficient Identification Schemes Using Two Prover Interactive Proofs*, Advances in Cryptography, CRYPTO 89, LNCS 435, Springer-Verlag, pp. 498–506, 1989.

33. R. Raz, A. Wigderson, *Monotone Circuits for Matching require Linear Depth*, Proc. of the 22nd STOC, pp. 287–292, May 1990.

34. Y. Gil, F. Meyer auf der Heide, A. Wigderson, *Not All Keys can be Hashed in Constant Time*, Proc. of the 22nd STOC, pp 244–253, May 1990.

35. S. Ben-David, A. Borodin, R. Karp, G. Tardos, A. Wigderson, *On the Power of Randomization in On-line Algorithms*, Proc. of the 22nd STOC, pp. 379–388, May 1990.

36. R. Heyman, I. Newman, A. Wigderson, *On Read-Once Threshold Formulae and their Randomized Decision Tree Complexity*, 5th Structures in Complexity Theory, pp. 78-89, July 1990.

37. I. Newman, P. Ragde, A. Wigderson, *Perfect Hashing, Graph Entropy and Circuit Complexity*, Proc. of the 5th Structures in Complexity Theory conference, pp. 91-99, July 1990.

38. P. Gemmel, R. Lipton, R. Rubinfeld, M. Sudan and A. Wigderson, *Self Testing / Correcting for Polynomials and for Approximate Functions*, Proc. of the 23rd STOC, pp. 32–42, May 1991.

39. N. Nisan and A. Wigderson, *Rounds in Communication Complexity Revisited*, Proc. of the 23rd STOC, pp. 419–429, May 1991.

40. R. Heiman and A. Wigderson, *Randomized vs. Deterministic Decision Tree Complexity for Read–Once Boolean Functions*, Proc. of the 6th Structures in Complexity Theory Conference, pp. 172-179, July 1991.

41. L. Babai, L. Fortnow, N. Nisan and A. Wigderson, *BPP has Subexponential Time Simulations unless EXPTIME has Publishable Proofs*, Proc. of the 6th Structures in Complexity Theory comference, pp. 213-219, July 1991.

42. M. Karchmer, R. Raz and A. Wigderson, *Super–Logarithmic Depth Lower Bounds via Direct Sum in Communication Complexity*, Proc. of the 6th Structures in Complexity Theory conference, pp. 299–304, July 1991.

43. Yu. Rabinovich and A. Wigderson, *An Analysis of a Simple Genetic Algorithm*, Proc. of the 4th International Conference on Genetic Algorithms, pp. 215-221, July 1991.

44. L. Lovasz, I. Newman, M. Naor, A. Wigdreson, *Search Problems in the Decision Tree Model*, Proc of the 32nd FOCS conference, pp. 576–585, 1991.

45. M. Karchmer, I. Newman, M. Saks, A. Wigderson, *Non– deterministic Communication Complexity with Few Witnesses*, 7th Structures in Complexity Theory conference, pp. 275–281, 1992.

46. N. Nisan, E. Szemeredi, A. Wigderson, *Undirected Connectivity in $O(\log^{1.5} n)$ Space*, Proc. of the 33rd FOCS conference, pp. 24–29, 1992.

47. Yu. Rabinovich, A. Sinclair, A. Wigderson, *Quadratic Dynamical Systems*, Proc. of the 33rd FOCS conference, pp. 24–27, 1992.

48. M. Karchmer, A. Wigderson, *On Span Programs*, Proc. of the 8th Structures in Complexity conference, pp. 102–111, 1993.

49. A. Wigderson, D. Zuckerman, *Expanders that Beat the Eigenvalue Bound, Explicit Construction and Applications*, Proc. of the 25th STOC, pp. 245–251, 1993.

50. M. Karchmer, A. Wigderson, *On Characterizing Nondeterministic Circuit Size*, Proc. of the 25th STOC, pp. 532–545, 1993.

51. M. Luby, B. Velickovic and A. Wigderson, Deterministic Approximate Counting of Depth–2 Circuits, Proc. of the 2nd ISTCS (Israeli Symposium on Theoretical Computer Science), pp. 18–24, 1993.

52. R. Ostrovski and A. Wigderson, *Nontrivial Zero-Knowledge implies One–Way Functions*, Proc. of the 2nd ISTCS, pp. 3–17, 1993.

53. O. Goldreich, A. Wigderson, *Tiny Families of Functions with Random Properties: A Quality–Size Trade–off*, Proc. of the 26th STOC, pp. 574–583, 1994.

54. R. Impagliazzo, N. Nisan, A. Wigderson, *Pseudorandomness for Network Algorithms*, Proc. of the 26th STOC, pp. 356–364, 1994.

55. A. Condon, L. Hellerstein, S. Pottle, A. Wigderson, *On the Power of Finite Automata with Both Nondeterministic and Probabilistic States*, Proc. of the 26th STOC, pp. 676–685, 1994.

56. R. Impagliazzo, R. Raz. A. Wigderson, *A Direct Product Theorem*, Proc. of the 9th Structures in Complexity conference, pp. 88–96, 1994.

57. A. Wigderson, *NL/poly $\subseteq$ $\oplus$L/poly*, Proc. of the 9th Structures in Complexity conference, pp. 59–62, July 1994.

58. N. Nisan, A. Wigderson, *A note on Rank vs. Communication Complexity*, Proc. of the 35th FOCS, pp. 831–836, 1994.

59. P. Miltersen, N. Nisan, S. Safra, A. Wigderson, *On Data Structures and Asymmetric Communication Complexity*, Proc. of the 27th STOC, pp. 103–111, 1995.

60. N. Nisan and A. Wigderson, *On the Complexity of Bilinear Forms*, Proc. of the 27th STOC, pp. 723–732, 1995.

61. N. Nisan and A. Wigderson, *Lower Bounds on Arithmetic Circuits via Partial Derivatives*, Proc. of the 36th FOCS, pp. 16–25, 1995.

62. I. Damgard, O. Goldreich, T. Okamoto and A. Wigderson, *Honest Verifier vs Dishonest Verifier in Public Coin Zero-Knowledge Proofs*, Advances in Cryptology – Crypto '95 (Proceedings), Lecture Note in Computer Science (963) Springer Verlag, pp. 325–338, 1995.

63. L. Babai, A. Gal, J. Kollar, L. Ronyai, T. Szabo, A. Wigderson, *Extremal Bipartite Graphs and Superpolynomial Lower Bounds for Monotone Span Programs*, Proc of 28th STOC, pp. 603–611, 1996.

64. R. Sharan, A. Wigderson, *A New NC Algorithm for Perfect Matching in Bipartite Cubic Graphs*, Proc. of ISTCS 96, pp. 56–65, 1996.

65. R. Armoni, M. Saks, A. Wigderson, S. Zhou, *Discrepancy Sets and Pseudorandom Generators for Combinatorial Rectangles*, Proc. of the 37th FOCS, pp. 412–421, 1996.

66. A. Razborov, A. Wigderson, A. Yao. *Read-Once Branching Programs, Rectangular Proofs of the Pigeonhole Principle and Transversal Calculus*, Proc. of the 29th STOC, pp. 739-748, 1997.

67. I. Parnafes, R. Raz, A. Wigderson, *Direct Product Results and the GCD Problem, in Old and New Communication Models* , Proc. of the 29th STOC, pp. 363–372, 1997.

68. R. Armoni, A. Ta-Shma, A. Wigderson, S. Zhou, $SL \subseteq L^{4/3}$, Proc. of the 29th STOCpp. 230–239, 1997.

69. R. Impagliazzo, A. Wigderson, *P=BPP unless E has Subexponential Circuits: Derandomizing the XOR Lemma*, Proc. of the 29th STOC, pp. 220–229, 1997.

70. H. Buhrman, R. Cleve, A. Wigderson, *Quantum vs. Classical Communication and Computation*, Proc. of 30th STOC, pp. 63–68, 1998.

71. N. Linial, A. Samorodnitsky, A. Wigderson, *A deterministic strongly polynomial algorithm for matrix scaling and approximate permanents*, Proc. of 30th STOC, pp. 644–652, 1998.

72. R. Impagliazzo, A. Wigderson, *Randomness vs. Time: De-randomization under a uniform assumption*, Proc. of the 39th FOCS, pp.734–743, 1998.

73. A. Ambainis, L. Schulman, A. Ta-Shma, U. Vazirani, A. Wigderson, *The Quantum Communication Complexity of Sampling*, Proc. of the 39th FOCS, pp. 342–351, 1998.

74. E. Ben-Sasson, A. Wigderson, *Short Proofs are Narrow – Resolution made Simple*, Proc. of the 31th STOC, pp. 517–526, 1999.

75. A. Shpilka, A. Wigderson, *Depth-3 Arithmetic Formulae over Fields of Characteristic Zero*, Proc. of the 14th Conference on Computational Complexity, pp. 87–97, 1999.

76. Z. Bar-Yossef, O. Goldreich, A. Wigderson, *Deterministic Amplification of Space-Bounded Probabilistic Algorithms* Proc. of the 14th Conference on Computational Complexity, pp. 188–199, 1999.

77. O. Goldreich, A. Wigderson, *Improved derandomization of BPP using a hitting set generator*, Proc. of the RAMDOM 99 Conference, pp. 131–137, 1999.

78. R. Impagliazzo, R. Shaltiel, A. Wigderson, *Near-optimal Conversion of Hardness into Pseudo-randomness*, Proc. of the 40th FOCS, pp. 181–190, 1999.

79. O. Goldreich, A. Wigderson, *On Pseudorandomness with respect to Deterministic Observers*, Proceedings of the satellite workshops of the 27th ICALP, Carleton Scientific (Proc in Informatics 8), pages 77–84, 2000.

80. O. Reingold, S. Vadhan, A. Wigderson, *Entropy Waves, The Zig-Zag Graph Product, and New Constant-Degree Expanders and Extractors*, Proc. of the 41st FOCS, pages 3–13, 2000.

81. M. Alekhnovich, E. Ben-Sasson, A. Razborov. A. Wigderson, *Pseudorandom Generators in Propositional Proof Complexity*, Proc. of the 41st FOCS, pages 43–53, 2000.

82. O. Reingold, R. Shaltiel, A. Wigderson, *Extracting Randomness via Repeated Condensing*, Proc. of the 41st FOCS, pages 22–31, 2000.

83. R. Impagliazzo, R. Shaltiel, A. Wigderson, *Extractors and Pseudo-random Generators with Optimal Seed Length*, Proc. of the 32nd STOC, 2000.

84. J. Hastad, A. Wigderson, *Simple Analysis of Graph Tests*, Conference on Computational Complexity, pages 244–255, 2001.

85. R. Impagliazzo, V. Kabanets, A. Wigerson, *In Search of an Easy Witness: Expential vs. Probablilistic Time*, Conference on Computational Complexity, pages 2–12, 2001.

86. O. Goldreich, S. Vadhan, A. Wigderson *On Interative Proofs with a Loconic Power*, Proc. of the 28th ICALP, 2001.

87. N. Alon, A. Lubotzky, A. Wigderson *Semi-direct product in groups and Zig-zag product in graphs: Connections and applications*, Proc. of the 42nd FOCS, 2001.

88. O. Goldreich, A. Wigderson *Derandomization that is Rarely Wrong from Short Advice that is Typically Good*, Randomization and Approximation Techniques in Computer Science, 6th International Workshop, RANDOM 2002, 209–223, 2002.

89. M. Capalbo, O. Reingold, S. Vadhan, A. Wigderson *Randomness Conductors and Constant-Degree Expansion Beyond the Degree/2 Barrier*, Proceedings of the 34th STOC, 659–668, 2002.

90. E. Friedgut, Kahn, A. Wigderson, *Computing Graph Properties by Randomized Subcube Partitions*, Randomization and Approximation Techniques in Computer Sciences, 6th International Workshop, RANDOM 2002, 105–113, 2002.

91. C-J Lu, O. Reingold, S. Vadhan, A. Wigderson *Extractors: Optimal up to Constant Factors*, 35th Annual ACM Symposium, STOC 2003, 602–611, 2003.

92. B. Barak, R. Shaltiel, A. Wigderson *Computational Analogues of Entropy*, 11th International Conference on Random Structures and Algorithms, RANDOM 2003, 200–215, 2003.

93. E. Ben-Sasson, M. Sudan, S. Vadhan, A. Wigderson *Randomness-efficient Low Degree Tests and Short PCPs via Epsilon-Biased Sets*, 35th Annual ACM Symposium, STOC 2003, 612-621, 2003.

94. E. Rozenman, A. Shalev, A. Wigderson *A New Family of Cayley Expanders(?)*, 36th Annual ACM Symposium, STOC 2004, 445–454, 2004.

95. A. Shpilka, A. Wigderson *Derandomizing homomorphism testing in general groups*, 36th Annual ACM Symposium, STOC 2004, 427–435, 2004.

96. B. Barak, R. Impagliazzo, A. Wigderson *Extracting randomness using few independent sources*, Proc of the 45th FOCS 2004, 384–393, 2004. SICOMP, vol. 36, no. 4, pp. 1095-1118, 2006.

97. B. Barak, G. Kindler, R. Shaltiel, B. Sudakov, A. Wigderson, *Simulating Independence: New Constructions of Condensers, Ramsey Graphs, Dispersers, and Extractors*, Proc. of the 46th STOC 2005, 1-10, 2005.

98. A. Wigderson, D. Xiao, *A randomness-efficient sampler for matrix-valued functions and applications*, Proceedings of the 46th Annual Symposium of FOCS 2005, pp. 397–406, 2005.

99. P. Beame, T. Pitassi, N. Segerlind, A. Wigderson, *A strong direct product theorem for corruption and the multiparty NOF communication complexity of set disjointness*, Proc. of CCC 2005, pp. 52-66, 2005.

100. I. Dinur, M. Sudan, A. Wigderson, *Robust local testability of tensor products of LDPC codes*, Proc. of RANDOM 2006, pp. 304-315, 2006.

101. B. Barak, A. Rao, R. Shaltiel, A. Wigderson, *2-Source Dispersers for Sub-Polynomial Entropy and Ramsey Graphs Beating the Frankl-Wilson Construction*, Proc. of STOC 2006, pp. 671–680, 2006.

102. A. Wigderson, *P, NP and Mathematics - a computational complexity perspective*, Proc. of the ICM 06 (Madrid), Vol. I, EMS Publishing House, Zurich, pp. 665–712, 2007.

103. E. Viola, A. Wigderson, *One-way multi-party communication lower bound for pointer jumping with applications*, Proc. of the FOCS 2007 conference, pp. 427–437, 2007.

104. Z. Dvir, A. Gabizon, A. Wigderson, *Extractors and rank extractors for polynomial sources*, Proc. of the FOCS 2007, pp. 52–62, 2007.

105. E. Viola, A. Wigderson, *Norms, XOR lemmas, and lower bounds for $GF(2)$ polynomials and multiparty protocols*, Proc. of the CCC 2007, pp. 141–154, 2007.

106. V. Guruswami, J. Lee, A. Wigderson, *Euclidean sections of l_1^N with sublinear randomness and error-correction over the reals*, Proc. of APPROX-RANDOM 2008, pp. 444-452, 2008.

107. S. Aaronson, A. Wigderson, *Algebrization: A New Barrier in Complexity Theory*, Proc. of STOC 2008, pp. 731-740, 2008.

108. G. Kindler, A. Rao, R. O'Donnell, A. Wigderson, *Spherical Cubes and Rounding in High Dimensions*, Proc. of FOCS 2008, pp. 189-198, 2008.

109. Z. Dvir, A. Wigderson, *Kakeya sets, new mergers and old extractors*, Proc. of FOCS 2008, pp. 625-633, 2008.

110. R. Impagliazzo, V. Kabanets, A. Wigderson, *New Direct-Product Testers and 2-Query PCPs*, Proc. of STOC 2009, 131-140, 2009.

111. A. Chattopadhyay, A. Wigderson, *Linear systems over composite moduli*, Proc. of FOCS 2009, pp. 43-52, 2009.

112. R. Impagliazzo, R. Jaiswal, V. Kabanets, A. Wigderson, *Uniform Direct Product Theorems: Simplified, Optimized, and Derandomized*, Proc. of STOC 08, pp. 579-588, 2008. SIAM J. Comput., vol. 39, no. 4, pp. 1637-1665, 2010.

113. S. Arora, D. Steurer, A. Wigderson, *Towards a study of low-complexity graphs*, Proc. of ICALP 2009, pp. 119-131, 2009.

114. B. Applebaum, B. Barak, A. Wigderson, *Public Key Cryptography from Different Assumptions*, Proc. of STOC 2010, pp. 171-180, 2010.

115. P. Hrubeš, A. Wigderson, A. Yehudayoff, *Non-commutative circuits and the sum-of-squares problem*, Proc. of STOC 2010, pp. 667-676, 2010.

116. P. Hrubeš, A. Wigderson, A. Yehudayoff, *Relationless completeness and separations*, Proc. of CCC 2010, pp. 280-290, 2010.

117. T. Kaufman, A. Wigderson, *Symmetric LDPC codes and local testing*, Proc. of ICS 2010, pp. 406-421, 2010.

118. P. Hrubeš, A. Wigderson, A. Yehudayoff, *Non-commutative circuits and the sum-of-squares problem*, Proc. of STOC 2010, pp. 667-676, 2010.

119. B. Barak, Z. Dvir, A. Wigderson, A. Yehudayoff, *Fractional Sylvester-Gallai theorems*, Proc. of the National Academy of Sciences of the United States of America 2012.

120. A. Wigderson, A. Yehudayoff, *Population Recovery and Partial Identification*, Proc. of FOCS 2012, pp. 390-399, 2012.

121. Z. Dvir, A. Rao, A. Wigderson, A. Yehudayoff, *Restriction Access*, Proc. of ITCS 2012, pp. 19-33, 2012.

122. D. Gavinsky, O. Meir, O. Weinstein, A. Wigderson, *Toward better formula lower bounds: An informaion complexity approach to the KRW composition conjecture*, Proc. of STOC 2014.

123. O. Goldreich, A. Wigderson, *On derandomizing algorithms that Err extremely rarely*, Proc. of STOC 2014.

124. P. Hrubeš, A. Wigderson, *Non-commutative arithmetic circuits with division*, Proc. of ITCS 2014, pp.49-66, 2014.

125. Z. Dvir, S. Saraf, A. Wigderson, *Breaking the quadratic barrier for 3-LCC's over the reals*, Proc. of STOC 2014, pp. 784-793, 2014.

126. T. Ma, A. Wigderson, *Sum-of-Squares Lower Bounds for Sparse PCA*, Neural Information Processing Systems, NIPS 2015, pp. 1612-1620, 2015.

127. R. Meka, A. Potechin, A. Wigderson, *Sum-of-squares lower bounds for planted clique*, Proc. of STOC 2015, pp. 87-96, 2015.

128. O. Goldreich, E. Viola, A. Wigderson, *On Randomness Extraction in ACo*, Proc. of CCC 2015, pp. 601-668, 2015.

129. P. Gopalan, N. Nisan, R. Servedio, K. Talwar, A. Wigderson, *Smooth Boolean functions are easy: efficient algorithms for low-sensitivity functions*, Proc. of ITCS 2016, pp. 59-70, 2016.

130. A. Garg, L. Gurvits, R. Oliveira, A. Wigderson, *A deterministic polynomial time algorithm for non-commutative rational identity testing*, Proc. of FOCS 2016, pp. 109-117, 2016.

131. M. Forbes, A. Shpilka, I. Tzameret, A. Wigderson, *Proof Complexity Lower Bounds from Alegbraic Circuit Complexity*, Proc. of CCC 2016, pp. 32:1-32:17, 2016.

132. P. Gopalan, R. Servedio, A. Wigderson, *Degree and Sensitivity: tails of two distributions*, Proc. of CCC 2016, pp. 13:1-13:23, 2016.

133. R. Gelles, B. Haeupler, G. Kol, N. Ron-Zewi, A. Wigderson, *Towards Optimal Deterministic Coding for Interactive Communication*, Proc. of SODA 2016, pp. 1922-1936, 2016.

134. Z. Allen-Zhu, Y. Li, R. Oliveira, A. Wigderson, *Much Faster Algorithms for Matrix Scaling*, Proc. of FOCS 2017, pp. 890-901, 2017.

135. P. Burgisser, A. Garg, R. Oliveira, M. Walter, A. Wigderson, *Alternating minimization, scaling algorithms, and the null-cone problem from invariant theory*, Proc. of ITCS 2018, pp. 24:1-24:20, 2018.

136. K. Efreminko, A. Garg, R. Oliveira, A. Wigderson, *Barriers for Rank Methods in Arithmetic Complexity*, Proc. of ITCS 2018, pp. 1:1-1:19, 2018.

15.3 Invited Papers:

1. A. Wigderson, *The Fusion Method for Lower Bounds in Circuit Complexity*, Combinatorics, Paul Erdös is Eighty (Vol. 1), Miklós, Sós and Szönyi (Eds.), Bolyai Math. Society, pp. 453–468, 1993.

2. A. Wigderson, *The Complexity of Graph Connectivity*, Proc. of the 17th Mathematical Foundations of Computer Science conference, Havel and Koubek (Eds.), Lecture Notes in Computer Science 629, Springer-Verlag, pp. 112–132, 1992.

3. A. Wigderson, *Information Theoretic Reasons for Computational Difficulty*, Proceedings of the International Congress of Mathematicians, pp. 1537–1548, August 1990.

15.4 Technical Reports:

1. A. Wigderson, *The Complexity of the Hamiltonian Circuit Problem for Maximal Planar Graphs*, Technical Report #298, Department of EECS, Princeton University, February 1982.

2. G. Vijayan, A. Wigderson, *Planarity of Edge Ordered Graphs*, Technical Report #307, Department of EECS, Princeton University, December 1982.