

ERDAL ARIKAN

Professor
Bilkent University
Electrical Engineering Dept.
TR-06533, Ankara, Turkey
(90)-312-2901347 (work), (90)-312-2664083 (home), (90)-532-211-8132 (mobile)
arikan@ee.bilkent.edu.tr

PROFESSIONAL INTERESTS

Information Theory and Coding, Communication Systems and Networks, Reconfigurable Hardware Implementation of Communications Systems.

EDUCATION

September 1982 – December 1985 *Massachusetts Institute of Technology, Cambridge, MA*
Ph.D. in Electrical Engineering and Computer Science
Thesis Title: Sequential Decoding for Multiple Access Channels
Supervisor: Prof. Robert G. Gallager
Minor in Probability and Stochastic Processes
GPA = 5.0 / 5.0

September 1981 – August 1982 *Massachusetts Institute of Technology, Cambridge, MA*
S.M. in Electrical Engineering and Computer Science
Thesis Title: Multi-Access in Packet Radio Networks
Supervisor: Prof. Robert G. Gallager
GPA = 5.0 / 5.0

September 1978 – June 1981 *California Institute of Technology, Pasadena, CA*
B.S. in Electrical Engineering
GPA = 4.0 / 4.0

AWARDS, ACHIEVEMENTS, PROFESSIONAL SERVICES

2010 Winner of IEEE Information Theory Society 2010 Paper Award for the paper "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels" published in July 2010 issue of the IEEE Transactions on Information Theory.

Sept 2004 — Sept 2007 Member of TUBITAK EEEAG Executive Committee.

1994, 2002, 2003, 2004 Member of Technical Program Committee, IEEE International Symposium on Information Theory

2000-2002 Region 8 Representative, IEEE Individual Benefits and Services Committee

1993-1995 Associate Editor-at-Large, IEEE Transactions on Information Theory

1994 IEEE Recognition as Founding Chairman of IEEE Communications Society, Turkey Chapter.

1994 Best Paper Award, European Simulation Symposium, 9-12 Sept. 1994, Istanbul. (Paper title 'A dynamic importance sampling method for quick simulation of rare events,' with A. Erdoğ an.)

1993 Elected Senior Member of IEEE

1993 AFCEA Honor Certificate for work in the simulation of military communication systems.

1981 – 1982 Vinton Hayes Fellowship in Communications, M.I.T.

1980 – 1981 Henry Ford II Scholar Award (awarded to senior with the highest GPA)

1976

First Place in the National University Entrance Examinations, Turkey.

WORK EXPERIENCE

September 1987 – present

Bilkent University, Ankara, Turkey

Professor in the Department of Electrical and Electronics Engineering. Courses Taught: Telecommunications, Computer Networks, Information Theory, Algebraic Coding Theory, Combinatorics, Probability, Random Processes, Quantum Computing and Communications.

January 1986 – August 1987

University of Illinois at Urbana-Champaign

Assistant Professor in the Department of Electrical and Computer Engineering. Research Assistant Professor in the Coordinated Science Laboratory.

RECENT PROJECT WORK

Feb 2008 – present

TBTAK Project – 107E216 "Channel polarization",

Role: Principal Investigator. Budget: 169,000 TL. Completion date: Jan 31, 2011.

Apr 2010 – present

INTEL Project – "Channel polarization for MIMO OFDM systems",

Role: Principal Investigator. Budget: 50,000 USD. Completion date: Mar 31, 2011.

Jan 2008 – present

NEWCOM++ – Network of Excellence on Wireless Communications,

European Union FP7 Project. Role: Principal Investigator for Bilkent. Budget: 72 KEuro per year. Completion date: December 2010.

Jan. 2008 – present

WiMAGIC – Worldwide Interoperability Microwave Broadband Access System for Next Generation Wireless Communications,

European Union FP7 STREP Project. Role: Researcher.

PUBLICATIONS

Journal Articles

- 1) S. Kyriakides and E. Arıkan, 'Postbuckling behavior of inelastic inextensional rings under external pressure,' *ASME J. Applied Mechanics*, 83-WA/APM-4, 1983.
- 2) E. Arıkan, 'Some complexity results about packet radio networks,' *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 681-85, July 1984.
- 3) —, 'An upper bound on the cutoff rate of sequential decoding,' *IEEE Trans. Inform. Theory*, vol. IT-34, pp. 55-63, Jan. 1988.
- 4) —, 'Sequential decoding for multiple access channels,' *IEEE Trans. Inform. Theory*, vol. IT-34, pp. 246-259, March 1988.
- 5) —, 'An implementation of Elias coding for input-restricted channels,' *IEEE Trans. Inform. Theory*, vol. IT-36, pp. 162-165, Jan. 1990.
- 6) —, 'On the achievable rate region of sequential decoding for a class of multiple access channels,' *IEEE Trans. Inform. Theory*, vol. IT-36, pp. 180-183, Jan. 1990.
- 7) B. Radosavljevic, B. Hajek, E. Arıkan, 'Sequential decoding with adaptive reordering of codeword trees,' *IEEE Trans. Inform. Theory*, vol. IT-38, no. 6, pp. 1833-1838, Nov. 1992.
- 8) E. Arıkan, 'A bound on the zero-error list-coding capacity,' *Coding and Quantization: IEEE/DIMACS Workshop, Oct. 19-21, 1992, Edited by A.R. Calderbank*.
- 9) —, 'An upper bound on the zero-error list-coding capacity,' *IEEE Trans. Inform. Theory*, vol. IT-40, no. 6, pp. 1237-1240, July 1994.
- 10) N. Akar and E. Arıkan, 'Markov modulated periodic arrival process offered to an ATM multiplexer,' *Performance Evaluation*, vol. 22, pp. 175-190, 1995.
- 11) E. Arıkan, 'An inequality on guessing and its application to sequential decoding,' *IEEE Trans. Inform.*

Theory, vol. IT-42, no. 1, pp. 99-105, Jan. 1996.

- 12) N. Akar and E. Arıkan, 'A numerically efficient method for the MAP/D/1/K queue via rational approximations,' *Queueing Systems*, vol. 22, pp. 97-120, Feb. 1996.
- 13) M. Abdelati and E. Arıkan, 'A scheme for handling connectionless services in connection-oriented networks,' *IEICE Trans. Communications*, vol. E80-B, no. 10, pp. 1514-1522, Oct. 1998.
- 14) E. Arıkan and N. Merhav, 'Guessing subject to distortion,' *IEEE Trans. Inform. Theory*, vol. IT-44, no. 3, pp. 1041-1056, May 1988.
- 15) E. Arıkan and N. Merhav, 'Joint source-channel coding and guessing with application to sequential decoding,' *IEEE Trans. Inform. Theory*, vol. IT-44, no. 5, pp. 1756-1769, Sept. 1998.
- 16) N. Merhav, R. M. Roth, and E. Arıkan, 'Hierarchical guessing with a fidelity criterion,' *IEEE Trans. Inform. Theory*, vol. IT-45, no. 1, pp. 330-337, Jan. 1999.
- 17) N. Merhav and E. Arıkan, 'The Shannon cipher system with a guessing wiretapper,' *IEEE Trans. Inform. Theory*, vol. IT-45, no. 6, pp. 1860-1866, Sept. 1999.
- 18) E. Arıkan, 'On the reliability exponent of the exponential timing channel,' *IEEE Trans. Inform. Theory*, vol. IT-48, no. 6, pp. 1681-1689, June 2002.
- 19) E. Arıkan, 'Channel combining and splitting for cutoff rate improvement,' *IEEE Trans. Inform. Theory*, vol. IT-52, no. 2, pp. 628-639, Feb 2006.
- 20) A. S. Tan, A. Aksay, G. B. Akar, and E. Arıkan, 'Rate-distortion optimization for stereoscopic video streaming with unequal error protection,' *EURASIP Journal on Advances in Signal Processing*, vol. 2008, DOI:10.1155/2008/632545.
- 21) E. Arıkan, 'A performance comparison of polar codes and Reed-Muller codes,' *IEEE Communications Letters*, vol. 12, no. 6, pp. 447-449, June 2008
- 22) E. Arıkan, 'Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input channels,' *IEEE Trans. Inform. Theory*, vol. 55, no. 7, pp. 3051-3073, Jul 2009.
- 23) A. Ozelikkale, H. M. Ozaktas, and E. Arıkan, 'Signal recovery with cost-constrained measurements,' *IEEE Trans. Signal Processing*, vol. 58, no. 7, pp. 3607-3617, Jul 2010.

Conference Publications

- 1) E. Arıkan, 'Sequential decoding for multiple access channels,' 1986 Int. Symp. Information Theory, p. 2, Ann Arbor, MI, Oct. 6-9, 1986.
- 2) E. Arıkan, 'A coding method for discrete noiseless channels with input constraints,' 1988 Int. Symp. Inform. Theory, p. 20, Kobe, Japan, June 19-24, 1988.
- 3) E. Arıkan, 'Trellis coding for high signal-to-noise ratio Gaussian noise channels,' *Conference Record MILCOM 89*, pp. 196-199, Boston, MA, Oct. 15-18, 1989.
- 4) E. Arıkan, 'Some results on zero-error capacity under list decoding,' 1990 Int. Symp. Inform. Theory, p. 15, San Diego, CA, Jan. 14-19, 1990.
- 5) E. Arıkan, 'Lower bounds to moments of list size,' 1990 Int. Symp. Inform. Theory, p. 145, San Diego, CA, Jan. 14-19, 1990.
- 6) E. Arıkan, 'A metric for sequential decoding on input-restricted channels,' *Proc. 1991 IEEE Int. Symp. Inform. Theory*, p. 294, Budapest, Hungary, June 24-28, 1991.
- 7) B. Radosavljevic, E. Arıkan, and B. Hajek, 'Sequential decoding with adaptive reordering of codeword trees,' *Proc. 1991 IEEE Int. Symp. Inform. Theory*, p. 292, Budapest, Hungary, June 24-28, 1991.
- 8) E. Arıkan, 'A bound on the zero-error list-coding capacity,' Joint IEEE/DIMACS Workshop on Coding and Quantization, Oct. 19-21, 1992, Rutgers University, NJ.
- 9) E. Arıkan, 'An upper-bound on the zero-error list-coding capacity,' 1993 Int. Symp. Inform. Theory, San Antonio.
- 10) N. Akar and E. Arıkan, 'Markov modulated periodic arrival process offered to an ATM multiplexer,'

IEEE Global Communications Conference, GLOBECOM'93, Nov. 29-Dec. 2, 1993, Houston TX.

- 11) N. Akar and E. Arıkan, 'Pade approximations in the analysis of the MMPP/D/1 system,' International Teletraffic Congress, ITC'93, Nov. 15-19, Bangalore, India.
- 12) E. Arıkan, 'An improved graph-entropy bound for perfect hashing,' *Proc. of Int. Symp. Inform. Theory*, p. 314, June 1994, Trondheim, Norway.
- 13) E. Arıkan, 'On the average number of guesses required to determine the value of a random variable,' *Trans. of the Twelfth Prague Conference on Information Theory, Statistical Decision Functions and Random Processes*, pp. 20-23, August 1994, Prague.
- 14) A. Erdođan and E. Arıkan, 'A dynamic importance sampling method for quick simulation of rare events,' *Proc. of the European Simulation Symposium*, pp. 63-67, October 1994, Istanbul.
- 15) M. Abdelati and E. Arıkan, 'A framework for the support of connectionless traffic over ATM networks,' *Proc. of The Ninth International Symposium on Computer and Information Sciences*, November 1994, Antalya.
- 16) E. Arıkan, 'An inequality on guessing and its application to sequential decoding,' *Proc. of IEEE Inform. Theory Symp.*, p. 322, Sept. 17-22, 1995, Whistler, CA.
- 17) M. Abdelati and E. Arıkan, 'Pricing of connectionless services in ATM networks,' *Proc. ISCIS X*, pp. 375-382, Kusadasi, Turkey, Oct. 30-Nov. 1, 1995.
- 18) M. Abdelati and E. Arıkan, 'A capital-asset pricing model approach for managing a connectionless virtual overlay network on top of an ATM network,' *Proc. Int. Conf. on Telecommunications, ICT'96*, Istanbul, April 13-17, 1996.
- 19) M. Abdelati and E. Arıkan, 'An approach to manage connectionless services in connection-oriented networks,' MELECOM 1996, Bari, May 13-16, 1996.
- 20) E. Arıkan and N. Merhav, 'Guessing subject to distortion,' *Proc. of IEEE Inf. Theory Workshop*, p. 64, June 13-16, 1996, Haifa, Israel.
- 21) N. Merhav and E. Arıkan, 'Guessing subject to distortion,' Workshop on Sequence Prediction, Santa Cruz, May 1997.
- 22) E. Arıkan and N. Merhav, 'Joint source-channel coding and guessing,' *Proc. of IEEE Inform. Theory Symp.*, p. 162, Ulm, Germany, June 29-July 4, 1997.
- 23) N. Merhav, R. M. Roth, and E. Arıkan, 'Hierarchical guessing with a fidelity criterion,' *Proc. of IEEE Inf. Theory Workshop*, San Diego, CA, Feb. 9-11, 1998.
- 24) N. Merhav and E. Arıkan, 'The Shannon cipher system with a guessing wiretapper,' *Proc. 1998 IEEE Int. Symp. Inform. Theory*, p. 83, Cambridge, MA, Aug. 16-21, 1998.
- 25) E. Arıkan, 'Large deviations of probability rank,' *Proc. 2000 IEEE Int. Symp. Inform. Theory*, p. 27, Sorrento, Italy, June 25-30, 2000.
- 26) G. Akkor and E. Arıkan, 'Improved bounds on convolutional code performance,' *Proc. 2001 IEEE Int. Symp. Inform. Theory*, p. 156, Washington D.C., June 24-29, 2001.
- 27) E. Arıkan, 'An information-theoretic analysis of Grover's algorithm,' *Proc. of NATO-ASI on Quantum Communication and Information Technologies*, June 3-14 Ankara, Turkey.
- 28) E. Arıkan and S. Boztas, 'Guessing with lies,' *Proc. 2002 IEEE Int. Symp. Inform. Theory*, p. 202, Lausanne, Switzerland, June 30-July 5, 2002.
- 29) E. Arıkan, 'On the reliability exponent of the exponential timing channel,' *Proc. 2002 IEEE Int. Symp. Inform. Theory*, p. 420, Lausanne, Switzerland, June 30-July 5, 2002.
- 30) E. Arıkan, 'An information theoretic analysis of Grover's algorithm,' *Proc. 2003 IEEE Int. Symp. Inform. Theory*, p. 401, Yokohama, Japan, June 29-July 4, 2003.
- 31) E. Arıkan, 'An information theoretic analysis of Grover's algorithm,' *Proc. 2003 IEEE Int. Symp. Inform. Theory*, p. 401, Yokohama, Japan, June 29-July 4, 2003.

- 32) R. Ahlswede, E. Arıkan, L. Baüıner, C. Deppe, 'Information theoretic models in language evolution,' *General Theory of Information Transfer and Combinatorics, (Report on a Research Project at the ZIF (Center for interdisciplinary studies) in Bielefeld, Oct. 1, 2002 - August 31, 2003, (Edited by R. Ahlswede, L. Baüıner, N. Cai.*
- 33) R. Ahlswede, E. Arıkan, L. Baüıner, C. Deppe, 'Language evolution and information theory,' Proc. 2004 IEEE Int. Symp. Inform. Theory, p. xxx, Chicago, IL, June 27-July 4, 2004.
- 34) E. Arıkan, 'Capacity bounds for ultra wideband channels,' Proc. 2004 IEEE Inform. Theory Workshop, ITW2004, San Antonio, TX, Oct. 24-29, 2004.
- 35) E. Arıkan, 'Channel combining and splitting for cutoff rate improvement,' Proc. 2005 IEEE Int. Symp. Inform. Theory, Adelaide, Australia, Sept. 4-9, 2005.
- 36) E. Arıkan, 'Guessing and cryptography,' Proceedings of NATO ASI on Network Security and Intrusion Detection, Nork, Yerevan, Armenia, Oct 2005.
- 37) E. Arıkan, 'Some remarks on the nature of the cutoff rate,' ITA Inaugural Workshop, UCSD, San Diego, Feb. 2006.
- 38) E. Arıkan, 'Time reversal signaling for ultra wideband communications,' Proceedings of Second International Symposium on Communications, Control, and Signal Processing, ICCSP'06, Marrakech, Morocco, March 2006.
- 39) E. Arıkan, 'Guessing and sequential decoding,' *Workshop on The Revival of Sequential Decoding*, Munich, Germany, May 2006.
- 40) O. Atak, A. Atalar, E. Arıkan, G. Ascheid, H. Meyr, M. Nicola, G. Masera, 'Design of application specific processors for the cached FFT algorithm', *2006 IEEE Int. Symp. Acoustics, Speech, and Signal Processing*, Toulouse, France, 14-19 May 2006.
- 41) O. Atak, A. Atalar, E. Arıkan, 'Cached fast Hartley transform algorithm and ASIP implementation,' *IST Mobile Summit 2006*, Myconos, Greece, 4-8 June 2006.
- 42) E. Arıkan, 'Wireless Network Security and Authentication,' *NATO Workshop on Network Security*, Almaty, Kazakhstan, June 2006.
- 43) H. Ishebabi, G. Ascheid, H. Meyr, O. Atak, A. Atalar, E. Arıkan, 'An efficient parallelization technique for high throughput FFT ASIPs' Proceedings of the 2006 International Symposium on Circuits and Systems, ISCAS 2006, Kos, Greece.
- 44) A. S. Tan, A. Aksay, C. Bilen, G. B. Akar, and E. Arıkan, 'Error resilient layered stereoscopic video streaming,' *Proceedings of 3DTV CON 2007, Capture, Transmission and Display of 3D Video*, 7-9 May 2007, Kos, Greece.
- 45) S. Argyropoulos, A. S. Tan, N. Thomos, E. Arıkan, and M. G. Strintzis, 'Robust transmission of multi-view video streams using flexible macroblock ordering and systematic LT codes,' *Proceedings of 3DTV CON 2007, Capture, Transmission and Display of 3D Video*, 7-9 May 2007, Kos, Greece.
- 46) A. S. Tan, A. Aksay, C. Bilen, G. B. Akar, Erdal Arıkan, 'Unequal error protection for stereoscopic video streaming,' *Proceedings of the IEEE 15th Signal Processing and Communications Applications Conference*, 11-13 June 2007, Eskisehir, Turkey
- 47) A. Ozcelikkale, H. M. Ozaktas, E. Arıkan, 'Measurement strategies for input estimation in linear systems,' *Proceedings of the IEEE 15th Signal Processing and Communications Applications Conference*, 11-13 June 2007, Eskisehir, Turkey.
- 48) A. Ozcelikkale, H. Ozaktas, E. Arıkan, 'Optimal measurement under cost constraints for estimation of propagating wave fields,' *Proceedings of 2007 IEEE International Symposium on Information Theory*, p. 61, 24-29 June 2007, Nice, France.
- 49) E. Arıkan and Y. Yapıcı, 'An improvement of the V-BLAST symbol detection algorithm for MIMO channels,' *Proceedings of Redundancy 2007*, 2-6 July 2007, St. Petersburg, Russia.
- 50) E. Arıkan, 'Channel polarization: a method for constructing capacity-achieving codes,' *Proceedings of 2008 IEEE International Symposium on Information Theory*, 6-11 July 2008, Toronto, Canada.

- 51) A. Serdar Tan, A. Aksay, G. B. Akar, and E. Arıkan, 'Stereoscopic video streaming with end-to-end modeling,' *Proc. 2008 IEEE 16th Signal Processing, Communications and Applications Conference*, pp. 541-544, Apr. 20-22, 2008, Aydın, Turkey.
- 52) E. Arıkan, H. Kim, G. Markarian, U. Özgür, E. Poyraz, 'Performance of short polar codes under ML decoding,' *ICT-Mobile Summit 2009*, June 10-12, 2009, Santander, Spain.
- 53) E. Arıkan and G. Markarian, 'Two dimensional polar coding,' *Tenth International Symposium on Coding Theory and Applications (ISCTA09)*, July 13-17, 2009, Ambleside, UK.
- 54) E. Arıkan and E. Telatar, 'On the rate of channel polarization,' *2009 IEEE Int. Symp. Inform. Theory*, 28 June - 3 July 2009, Seoul, South Korea.
- 55) E. Şaşoğlu, E. Telatar, E. Arıkan, 'Polarization for arbitrary discrete memoryless channels,' *2009 IEEE Information Theory Workshop (ITW 2009)*, October 11-16, 2009, Taormina, Sicily, Italy.
- 56) S. Ali, G. Markarian, and E. Arıkan, 'Novel Predistortion Algorithm for OFDMA,' *Proc. 69th IEEE Vehicular Technology Conference*, pp. 1447-1451, Apr. 26-29, 2009, Barcelona, Spain.
- 57) E. Arıkan, 'A survey of Reed-Muller codes from polar coding perspective,' *2010 IEEE Information Theory Workshop (ITW 2010)*, January 6-8, 2010, Cairo, Egypt.
- 58) M. Pilancı, O. Arıkan ve E. Arıkan, 'Kutupsal Sıkıştırma Örnekleme: Kutuplaşma Kodları ile Yeni Bir Yöntem,' *IEEE. 18. Sinyal İşleme ve İletişim Uygulamaları Kurultayı*, 22-24 Nisan 2010, Diyarbakır.
- 59) E. Arıkan, 'Source Polarization,' *Int. Symp. Information Theory*, June 13-18, 2010, Austin, TX.
- 60) E. Arıkan, 'Polar codes: A pipelined implementation,' *Proc. Int. Symp. Broadband Communication (ISBC2010)*, 11-14 July 2010, Melaka, Malaysia.

Edited Volume

E. Arıkan (editor), *Proceedings of the 1990 Bilkent International Conference on Communication, Control, and Signal Processing*. Elsevier: Amsterdam, 1990.

Plenary Talks

E. Arıkan, 'Kutuplama: Kapasiteye erien kodlar inas iin bir yntem,' 18. SIU Konferans, 22-24 Nisan 2010, Diyarbakır, Turkey.

E. Arıkan, 'A historical account of polar coding,' *Plenary Talk, IEEE Information Theory Workshop (ITW 2010 Dublin)*, Aug. 30 - Sept. 3, 2010, Dublin, Ireland.

E. Arıkan, 'From sequential decoding to polar codes,' *Plenary Talk, 6th International Symposium on Turbo Codes and Iterative Information Processing*, 6-10 September 2010, Brest, France.

E. Arıkan, 'Source and channel polarization,' *Plenary Talk, 2011 IEEE Int. Symp. Information Theory (ISIT 2011)*, Jul. 31 - Aug. 5, 2011, Saint Petersburg, Russia.

PERSONAL BACKGROUND

Born July 18, 1958 in Ankara, Turkey. Fluent in Turkish, English, Russian. Intermediate level German.

Brief biography and publications list - Ian F. Blake

Brief biography:

Ian F. Blake received his undergraduate education at Queen's University in Kingston, Ontario and his Ph.D. at Princeton University in New Jersey. From 1967 to 1969 he was a Research Associate with the Jet Propulsion Laboratories in Pasadena, California. From 1969 to 1996 he was with the Department of Electrical and Computer Engineering at the University of Waterloo, in Waterloo, Ontario where he was Chairman from 1978 to 1984 and Director of the Institute of Computer Research from 1990 to 1994. From 1996-1999 he was with the Hewlett-Packard Labs in Palo Alto, California. From 1999 to 2007 he was with the Department of Electrical and Computer Engineering at the University of Toronto. Since 2007 he has been an Honorary Professor in the Departments of Mathematics and Electrical and Computer Engineering at the University of British Columbia.

He has spent sabbatical leaves with the IBM Thomas J. Watson Research Center, the IBM Research Laboratories in Switzerland and M/A-Com Linkabit in San Diego, California. His research interests are in the areas of cryptography, algebraic coding theory, digital communications and spread spectrum systems.

He is a Fellow of the IEEE, a Fellow of the Royal Society of Canada, and a Fellow of the Canadian Academy of Engineering.

IEEE related activities:

Member of the Information Theory and Communication Societies; Two terms, Board of Governors, Information Theory Society, (President 1989); General Co-Chairman of the 1983 International Symposium on Information Theory; Technical Program Chair, 1995 International Symposium on Information Theory; Member of the Program Committees and International Committees of several IEEE Symposia and Conferences; Member of the IEEE Hamming Medal Committee, 1990-1994, (Chairman, 1992-1994); Member of the IEEE Awards Board, 1992-94; Member of the IEEE Technical Activities Board, 1989; Associate Editor, IT Transactions, Coding theory, 1997-2000.

Publications:

Books:

I.F. Blake (editor), *Algebraic Coding Theory - History and Development*, Dowden, Hutchison and Ross, Stroudsburg, PA, 1973.

I.F. Blake and R.C. Mullin, *The Mathematics of Coding Theory*, Academic Press, New York, NY, 1975. (The first three chapters of this book appeared also in a soft covered version entitled *An Introduction to Algebraic and Combinatorial Coding Theory*, 1976).

B.J. Walker and I.F. Blake, *Computer Security and Protection Structures*, Dowden, Hutchison and Ross, Stroudsburg, PA, 1976 (translated into Russian).

I.F. Blake, *An Introduction to Applied Probability*, John Wiley and Sons, New York, NY, 1979.

I.F. Blake and H.V. Poor, editors, *Communications and Networks: A Survey of Recent Advances* Springer-Verlag Inc., New York, NY, 1986.

Alfred J. Menezes, Ian F. Blake et al, *Applications of Finite Fields*, Kluwer Academic Publishers, Massachusetts, 1993.

Ian F. Blake, Gadiel Seroussi and Nigel P. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press, May, 1999.

Ian F. Blake, Gadiel Seroussi and Nigel P. Smart (eds.), *Advances in Elliptic Curve Cryptography*, Cambridge University Press, 2005.

Contributions to Books:

Ian F. Blake, Paul van Oorschot and Scott A. Vanstone, Complexity issues for public key cryptography, Chapter in *Performance Limits in Communication*, J.K. Skwirzynski ed., Martinus Nijhof, Holland, 1987.

Ian F. Blake, Coding for interference channels, Chapter 10 in *Communications and Networks: A Survey of Recent Advances*, Ian F. Blake and Vincent Poor eds., Springer-Verlag Inc., New York, NY, 1986.

Ian F. Blake, Peter Stublely and George H. Freeman, Enumeration of dyadic distributions, *Sequences '91*, Springer-Verlag Inc., New York, NY, 1992.

Ian F. Blake and Paul H. Wittke, Modulation and Coding for Digital Communications, *Encyclopedia for Telecommunications*, F.E. Froehlich ed., Marcel Dekker, Pittsburgh, Pa., 299-328, 1994.

Tomik Yaghoobian and Ian F. Blake, Reed-Solomon and Algebraic Geometry Codes, Chapter in *Reed-Solomon Codes*, V.K. Bhargava and S. Wicker eds., IEEE Press, 292-314, 1994.

Ian F. Blake, Shuhong Gao and Robert J. Lambert, Construction and distribution problems for irreducible trinomials over finite fields, in *Applications of Finite Fields*, D. Gollman, editor, Oxford: Oxford University Press, 1996.

Ian F. Blake, Curves, codes and cryptography, in *Codes, curves and signals: Common threads in communications*, A. Vardy editor, Dordrecht: Kluwer Academic Press, 1998.

Ian F. Blake, Cryptography, *Wiley Encyclopedia of Telecommunications*, John G. Proakis ed., 2002.

Ian F. Blake, Low density parity check codes, invited chapter in "CRC Press, 2nd Edition of the Handbook of Combinatorial Designs (2007).

Journal Articles:

I.F. Blake and J.B. Thomas, On a class of processes arising in linear estimation theory, *IEEE Trans. Inform. Theory*, Vol. IT-14, pp. 12-16, 1968.

I.F. Blake and J.B. Thomas, The linear random process, *Proc. IEEE*, Vol. 56, pp. 1696-1703, 1968.

I.F. Blake, Linear filtering and piecewise linear correlation functions, *IEEE Trans. Inform. Theory*, Vol. IT-15, pp. 345-349, 1969.

I.F. Blake, The Leech lattice as a code for the Gaussian channel, *Information and Control*, pp. 66-74, 1971.

D.Z. Djokovic and I.F. Blake, An optimization problem for unitary and orthogonal representations of finite groups, *Trans. Amer. Math. Soc.*, Vol. 164, pp.267-274, 1972.

I.F. Blake, Codes over certain rings, *Information and Control*. Vol. 20, pp.396-404, 1972.

I.F. Blake, Distance properties of group codes for the Gaussian channel, *SIAM Journal on Applied Mathematics*, pp. 312-324, 1972.

- I.F. Blake and W.C. Lindsey, Level crossing problems for random processes, *IEEE Trans. Inform. Theory*, Vol. IT-19, pp. 295-315, 1973.
- I.F. Blake and J.H. Gilchrist, Addresses for graphs, *IEEE Trans. Inform. Theory*, Vol. IT-19, pp. 683-688, 1973.
- I.F. Blake, Configuration matrices of group codes for the Gaussian channel, *IEEE Trans. Inform. Theory*, Vol. IT-20, pp. 95-100, 1974.
- I.F. Blake, Permutation codes for the discrete channel, *IEEE Trans. Inform. Theory*, Vol. IT-20, pp. 138-140, 1974 (Corresp.).
- I.F. Blake, Codes over integer residue rings, *Information and Control*, Vol. 29, pp. 295-300, 1975.
- J.J. Stiffler and I.F. Blake, An infinite class of generalized Room squares, *Discrete Mathematics*, Vol. 12, pp. 150-164, 1975.
- I.F. Blake, On a generalization of the Pless symmetry codes, *Information and Control*, Vol. 27, pp. 369-373, 1975.
- M. Rahman and I.F. Blake, Majority logic decoding using combinatorial designs, *IEEE Trans. Inform. Theory*, Vol. IT-21, pp. 585-587, 1975 (Corresp.).
- I.F. Blake and J.J. Stiffler, A construction method for generalized Room squares, *Aequationes Mathematicae*, Vol. 14, pp. 83-94, 1976.
- I.F. Blake and M. Rahman, A note on generalized Steiner systems, *Utilitas Mathematica*, Vol. 9, pp. 339-346, 1976.
- M. Rahman and I.F. Blake, Combinatorial aspects of orthogonal parity checks, *IEEE Trans. Inform. Theory*, Vol. IT-22, pp. 759-763, 1976 (Corresp.).
- M. Rahman and I.F. Blake, Combinatorial constructions of unequal error protection codes, *Utilitas Mathematica*, Vol. 11, pp. 215-225, 1977.
- I.F. Blake and A.G. Konheim, Big buckets are (are not) better, *Jour. ACM*, Vol. 24, pp. 591-606, 1977.
- I.F. Blake and J.J. Stiffler, A note on generalized Room squares, *Discrete Mathematics*, Vol. 21, pp. 89-93, 1978.
- I.F. Blake and A. Melkman, A note on the inverse of sections of the binomial matrix, *Discrete Mathematics*, Vol. 23, pp. 97-104, 1978.
- R. Safavi-Naini and I.F. Blake, On designs from codes, *Utilitas Mathematica*, Vol. 14, pp. 49-63, 1978.
- I.F. Blake and I. Gibson, Decoding the Golay code with miracle octad generators, *IEEE Trans. Inform. Theory*, Vol. IT-24, pp. 261-264, 1978 (Corresp.).
- I.F. Blake, Codes and designs, *Mathematics Magazine*, Vol. 52, pp. 81-95, 1979.
- I.F. Blake, G. Cohen and M. Deza, Coding with permutations, *Information and Control*, Vol. 43, pp. 1-19, 1979.
- R. Safavi-Naini and I.F. Blake, Generalized t-designs and orthogonal arrays, *Ars Combinatoria*, Vol. 7, pp. 135-151, 1979.
- R. Safavi-Naini and I.F. Blake, Generalized t-designs and weighted majority decoding, *Information and Control*, Vol. 42, pp. 261-282, 1979.
- I.F. Blake, The enumeration of certain run length sequences, *Information and Control*, Vol. 55, pp. 222-237, 1982.

- I.F. Blake, Performance of nonorthogonal signalling on an asynchronous multiple access on-off channel, *IEEE Trans. Communications*, Vol. COM-30, pp. 293-298, 1982 (Corresp.).
- I.F. Blake and J.W. Mark, A note on complex sequences with low correlation, *IEEE Trans. Inform. Theory*, Vol. IT-28, pp. 814-816, 1982 (Corresp.).
- G. Stuber, J.W. Mark and I.F. Blake, Sequence acquisition using bit estimation techniques, *Information Sciences*, Vol. 32, pp. 217-229, 1984.
- J.W. Mark and I.F. Blake, Rapid acquisition techniques in CDMA spread-spectrum systems, *IEE Proc.*, Vol. 131, Part F, pp. 223-232, 1984.
- I.F. Blake, R. Fuji-Hara, R.C. Mullin and S.A. Vanstone, Computing Logarithms in finite fields of characteristic two, *SIAM J. Alg. Disc. Meth.*, Vol. 5, pp. 276-285, 1984.
- Gordon L. Stuber, Ian F. Blake and Jon W. Mark, Performance of adaptive transmission on jammed fading channels, *IEEE Journal on Selected Areas in Communications*, Vol. SAC-5, pp. 176-187, 1987.
- Gordon L. Stuber, Jon W. Mark and Ian F. Blake, Diversity and coding for FH/MFSK systems with fading and jamming, Part 1: Multichannel diversity, *IEEE Trans. Communications*, Vol. COM-35, pp. 1329-1341, 1987.
- I. F. Blake and H. Darabian, Approximations for the probability in the tails of the binomial distribution, *IEEE Trans. Information Theory*. Vol. IT-33, pp. 426-428, 1987 (Corresp.).
- George Freeman, Jon W. Mark and Ian F. Blake, Trellis source codes designed by conjugate gradient optimization, *IEEE Trans. Communications*, Vol. COM-36, pp. 1-12, 1988.
- George Freeman, Ian F. Blake and Jon W. Mark, Trellis source code design as an optimization problem, *IEEE Trans. Inform. Theory.*, Vol. IT-34 (Part II), pp. 1226-1241, 1988.
- Benny C.Y. Wong and Ian F. Blake, Detector relative efficiency in non-Gaussian noise, *Journal of the Franklin Institute*, Vol 325, pp. 755-774, 1988.
- Gordon L. Stuber, Jon W. Mark and Ian F. Blake, An adaptive rate algorithm for FH/BFSK signaling, *IEEE Trans. Communications*, Vol. COM-36, pp.1269-1276, 1988.
- David W. Ash, Ian F. Blake and Scott A. Vanstone, The construction of low complexity normal bases, *Discrete Applied Mathematics.*, Vol. 25, pp. 191-210, 1989.
- Gordon L. Stuber, Jon W. Mark and Ian F. Blake, Diversity and coding for FH/MFSK systems with fading and jamming, Part 2: Selective diversity, *IEEE Trans. Communications*, Vol. COM-37, pp. 859-869, 1989.
- G.E. Atkin and Ian F. Blake, Performance of multitone FFH/MFSK systems in the presence of jamming, *IEEE Trans. Inform. Theory.*, Vol. IT-35, pp. 428-435, 1989.
- Benny C.Y. Wong and Ian F. Blake, An algorithm for the design of generalized quantizers for detection, *IEEE Trans. Communications*, Vol. 38, pp. 1384-1390, 1990.
- Klas Forsberg and Ian F. Blake, The enumeration of constrained sequences, *Jour. Computing and Information*, Vol. 1, pp.33-43, (1990).
- Muzhong Wang and Ian F. Blake, Bit serial multiplication in finite fields, *SIAM J. Disc. Math.*, Vol. 3, pp.140-148, 1990.
- Ian F. Blake and Khun Kith, On the complete weight enumerator of Reed-Solomon codes, *SIAM J. Disc. Math.*, Vol. 4, pp.164-171, 1991.

- Ian F. Blake, A perspective on coding theory, *Information Sciences*, Vol. 57-58, pp.111-118, 1991 (Invited paper).
- Vijay K. Bhargava, Ian F. Blake and L. Mason, Coding, diversity and minimum distance, *Can. Jour. Elec. Eng.*, Vol. 16, pp.87-92, (1991).
- Tomik Yaghoobian and Ian F. Blake, Hermitian codes as Reed-Solomon codes, *Designs, Codes and Cryptography*, vol. 2, pp.5-17, 1992.
- Ian F. Blake, S. Gao and R.C. Mullin, Explicit factorization of $x^{2^t} + 1$ over F_p with p prime $p \equiv 3 \pmod{4}$, *AAECC*, Vol. 4, pp.89-94, 1993.
- A.H. Baartmans, Ian F. Blake and V. Tonchev, On the extendability of t-designs, *Jour. Comb. Designs*, Vol. 1, 239-247, 1993.
- Benny C.Y. Wong and Ian F. Blake, Detection in multivariate non-Gaussian noise, *IEEE Trans. Comm.* Vol.42, pp.1672-1683, 1994.
- Ian F. Blake, S. Gao and R.C. Mullin, Normal and self-dual normal bases from factorization of $cx^{q+1} + dx^q - ax - b$, *SIAM J. Disc. Math.*, Vol. 7, pp. 499-512, 1994.
- Tomik Yaghoobian and Ian F. Blake, Two new decoding algorithms for Reed-Solomon codes, *AAECC*, Vol. 5, pp. 23-43, 1994.
- M. Alencar and Ian F. Blake, The capacity for a discrete state code division multiple access channel, *IEEE Journ. Sel. Areas of Comm.*, Vol. 12, pp.925-937, 1994.
- D. Dabiri and Ian F. Blake, Fast parallel algorithms for decoding Reed-Solomon codes based on remainder polynomials, *IEEE Trans. Inform. Theory*, Vol. 41, pp. 873-885, 1995.
- C.J. Wein and Ian F. Blake, On the performance of fractal compression with clustering, *IEEE Trans. Image Processing*, Vol. 5, pp. 522-526, 1996.
- V. Tarokh and Ian F. Blake, Trellis complexity versus the coding gain of lattices I, *IEEE Trans. Inform. Theory*, Vol. 42, pp. 1796-1807, 1996.
- V. Tarokh and Ian F. Blake, Trellis complexity versus the coding gain of lattices II, *IEEE Trans. Inform. Theory*, Vol. 42, pp. 1808-1816, 1996.
- V. Tarokh and Ian F. Blake, On the trellis complexity of the densest lattice packings in R^n , *SIAM J. Disc. Math.*, Vol. 9, pp. 597-601, 1996.
- Ian F. Blake, S. Gao and Ronald C. Mullin, Specific irreducible polynomials with linearly independent roots over finite fields, *Linear Algebra and its Applications*, Vol. 253, pp. 227-249, 1997.
- Muzhong Wang and Ian F. Blake, Normal basis of the finite field $F_{2^{(p-1)p^m}}$ over F_2 , *IEEE Trans. Inform. Theory*, Vol. 43, pp. 737-739, 1997.
- Cecilio Pimentel and Ian F. Blake, Modeling burst channels using partitioned Fritchman's Markov models, *IEEE Trans. Vehicular Tech.*, Vol. 47, pp. 885-899, 1998.
- Cecilio Pimentel and Ian F. Blake, Concatenated coding performance for FSK modulation onetime correlated Rician fading channels, *IEEE Trans. Communications*, Vol. 46, pp. 1610-1618, 1998.
- Shraga I. Bross and Ian F. Blake, Upper bound for uniquely decodable codes in a binary input N-user adder channel, *IEEE Trans. Inform. Theory*, Vol. 44, pp. 334-340, 1998.
- A.H. Banihashemi and Ian F. Blake, Trellis complexity and minimal trellis diagrams of lattices, *IEEE Trans. Inform. Theory*, Vol. 44, pp. 1829-1847, 1998.

- Huapeng Wu, M. Amwarul Hasan and Ian F. Blake, Low complexity bit-parallel finite field multipliers using weakly dual bases, *IEEE Trans on Computers*, Vol. 47, pp. 1223-1234, 1998.
- Ian F. Blake, Chris Heegard, Tom Høholdt and Victor Wei, Algebraic geometry codes, *IEEE Trans. Inform. Theory*, Vol. 44, pp. 2596-2618, 1998 (invited paper).
- Cecilio Pimentel and Ian F. Blake, Enumeration of Markov chains and burst error statistics for finite state channel models, *IEEE Trans. Vehicular Tech.*, Vol. 48, pp. 415-428, 1999.
- A.H. Banihashemi and Ian F. Blake, On the trellis complexity of root lattices and their duals, *IEEE Trans. Inform. Theory*, Vol. 45, pp. 2168-2172, 1999.
- Ian F. Blake and Theo Garefalakis, On the security of the DSA algorithm, *Designs, Codes and Cryptography*, Vol. 26, pp. 87-96 2002.
- H. Wu, A. Hasan, Ian F. Blake and Shuhong Gao, Finite field multipliers using redundant representations, *IEEE Trans. Computers*, Vol. 51, pp. 1306-1316, 2002 (Trans. Briefs).
- Ian F. Blake and Theo Garefalakis, On the complexity of the discrete logarithm and Diffie-Hellman problems, *J. Complexity*, vol. 20, 148-170, 2004.
- Ian F. Blake, V. Kumar Murty and Guangwu Xu, Efficient algorithms for curves $y^2 = x^3 - x - (-1)^a$ over field F_{3^m} , *Journal of Discrete Algorithms*, vol. 3, no. 1, pp. 113-124 (2005).
- Ian F. Blake, V. Kumar Murty and Guangwu Xu, A note on window τ -NAF algorithm, *Information Processing Letters*, v. 95, pp. 496-502 (2005).
- Kenneth Shum and Ian F. Blake, Expander graphs and codes, *AMS-DIMACS volume on Algebraic Coding Theory and Information Theory*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 68, pp. 57-68 (2005)
- Mehrdad Shamsi, Masoud Ardakani and Ian F. Blake, Mixed-Q linear space-time codes, *IEEE Transaction on Communications*, Vol. 54, no. 5, pp. 849-857, 2006.
- E.C. Park and Ian F. Blake, On the mean number of encryptions for tree-based broadcast encryption schemes, *Journal of Discrete Algorithms*, vol. 4, no. 2, pp. 215-238, 2006.
- Ian F. Blake, V. Kumar Murty and Guangwu Xu, Refinements of Miller's algorithm for computing the Weil/Tate pairing, *J. Algorithms*, vol 58, no. 2, pp. 134-149, Feb. 2006.
- Ian F. Blake, Theo Garefalakis and Igor Shparlinksi, On the Bit Security of the Diffie-Hellman Key, *Applicable Algebra in Communications and Computers*, vol. 16, no. 6, pp.397-404 2006.
- Ian F. Blake and Igor Shparlinksi, Statistical Distribution and Collisions of the VSH, *Journal of Mathematical Cryptology*, vol. 1, pp. 329-349, 2007.
- Ian F. Blake, V. Kumar Murty and Guangwu Xu, Nonadjacent radix- τ expansions of integers in Euclidean imaginary quadratic number fields, *Canadian Journal of Mathematics*, vol. 60, no. 6, pp. 1267-1282, 2008.
- Ian F. Blake and Theo Garefalakis, Polynomial approximation of the tripartite Weil-Diffie-Hellman map, *Finite Fields and their Applications*, vol. 14, pp. 379-389 2008.
- E.C. Park and Ian F. Blake, Construction of extended quadruple systems for information retrieval, *Revista Matematica Comput.*, vol. 21, no. 1, pp. 179-198, 2008.
- Chris Studholme and Ian F. Blake, Random matrices and codes for the erasure channel, accepted *Algorithmica*, 31 March, 2008, to appear.

- Omran Ahmadi, Noga Alon, Ian F. Blake and Igor Shparlinski, Graphs with integral spectra, *Linear Alg. Applns.*, vol. 430, no. 1, pp. 547-552, 2009.
- Ian F. Blake and Vladimir Kolesnikov, One round secure comparison of encrypted integers, *Journal of Mathematical Cryptology*, vol. 3, pp. 37-68, 2009.
- Ehsan Vahedi, Vincent Wong and Ian F. Blake, A note on a probabilistic analysis of an accurate tag estimation method, submitted to IEEE Transactions on Automation Science and Engineering (May 3, 2010).
- Ehsan Vahedi, Vahid Shah-Mansouri, Vincent Wong, Ian F. Blake, Probabilistic analysis of blocking attack in RFID systems, submitted.
- Ian F. Blake and Theo Garefalakis, On a transform property of Kloosterman sums, *Discrete Applied Mathematics*, accepted 2009.
- M. Khabbaziyan, Ian F. Blake and Vijay K. Bhargava, Local broadcast algorithms in wireless ad hoc networks: Reducing the number of transmissions, submitted to *IEEE Trans. Computers*, revised July, 2010.
- M. Khabbaziyan, Ian F. Blake and Vijay K. Bhargava, On improving key pre-distribution schemes for sensor networks, submitted.
- A. Nasri, R. Schober and Ian F. Blake, Performance and optimization of amplify-and forward cooperative diversity systems in generic noise and interference, accepted *IEEE Trans. Wireless Communications*, September 2010.
- Li Zhang, Qin Huang, Shu Lin, Khaled Abdel-Ghaffar, and Ian Blake, Quasi-Cyclic LDPC Codes: An Algebraic Construction, Rank Analysis and Codes on Latin Squares, accepted, *IEEE Trans. Communications*, 2010.
- Conference Papers:*
- I.F. Blake and J.B. Thomas, Applications of the linear random process, Hawaii International Conference on System Science, 1968.
- I.F. Blake and R.S. Jones, Noncyclic linear codes of length pq , Fifth Annual Princeton Conference on Information Sciences and Systems, 1971.
- I.F. Blake. Configuration matrices of group codes for the Gaussian channel, Sixth Annual Princeton, Conference on Information Sciences and Systems, 1972.
- I.F. Blake, Properties of generalized Pless codes, Twelfth Annual Allerton Conference on Circuit and System Theory, 1974.
- M. Rahman and I.F. Blake, Combinatorial decoding of certain codes, Twelfth Annual Allerton Conference on Circuit and System Theory, 1974.
- I.F. Blake, Group characters and representations in coding, Spring Meeting of the American Mathematical Society, Champaign-Urbana, Illinois, March, 1976, (Invited Address, abstracted in Notices of the AMS, February, 1976).
- I.F. Blake, Coding and t -designs, 83rd Annual Meeting of the American Mathematics Society, St. Louis, Missouri, January, 1977, (Invited Address, abstracted in Notices of the AMS, January, 1977).
- P.V. Bates and I.F. Blake, Radix two fast Fourier transform algorithms, Annual Princeton Conference on Information Sciences and Systems, 1980.

- I.F. Blake and J.W. Mark, A subsequence correlation approach to rapid acquisition for CDMA spread spectrum communication, Tenth Biennial Symposium on Communications, Queen's University, Kingston, May, 1980.
- G. Freeman, J. Mark and I.F. Blake, Performance of joint source and channel trellis codes, Canadian Communications and Energy Conference, October, 1982.
- I.F. Blake, R. Fuji-Hara, R.C. Mullin and S.A. Vanstone, Computing logarithms in finite fields of characteristic two, SIAM Second Conference on the Applications of Discrete Mathematics, Cambridge, MA, 1983.
- G.L. Stuber, I.F. Blake and J.W. Mark, Performance of coded spread spectrum systems over fading jamming channels, Twelfth Biennial Symposium on Communications, Queen's University, Kingston, June, 1984.
- I.F. Blake and J.W. Mark, Fast FH/MFSK with partial band and tone jamming, Twelfth Biennial Symposium on Communications, Queen's University, Kingston, June, 1984.
- I.F. Blake, R.C. Mullin and S.A. Vanstone, Discrete logarithms in $GF(2^n)$, Crypto '84, Santa Barbara, California, August, 1984. (Also appears in the conference proceedings, published in book.)
- G. Atkin and I.F. Blake, Performance of multitone FFH/MFSK Spread Spectrum System in the presence of multitone jamming, URSI Conference, North American Radio Science Meeting, Commission C, Vancouver, British Columbia, August, 1985.
- B.C.Y. Wong and Ian F. Blake, An algorithm for the design of generalized quantizer-detectors using independent noise samples, Princeton Conference of Information Systems and Sciences, Princeton, New Jersey, March, 1986.
- Gordon L. Stuber, Jon W. Mark and Ian F. Blake, Performance of FH/MFSK with diversity and coding versus a partial band jammer, 5th Annual Phoenix Conference on Computers and Communications, Phoenix, Arizona, March, 1986.
- Guillermo E. Atkin and Ian F. Blake, Optical communications using constant weight codes, International Symposium on Information Theory, Ann Arbor, Michigan, October, 1986.
- Ian F. Blake, Bases and computation in a finite field, Conference Internationale sur le Traitement d'Information et la Gestion d'Incertitudes dans les Systemes a Base de Connaissances, Paris, France, July, 1986.
- G. Stuber, I.F. Blake and J. Mark, An adaptive rate algorithm for FH/BFSK signaling, ICC 87, Seattle, Washington, June, 1987.
- Ian F. Blake, Properties of a class on nonbinary convolutional codes, Johns Hopkins Conf. on Inf. Systems and Science, March, 1987, Baltimore, MD.
- B. Wong and Ian F. Blake, Applications of series approximation to relative efficiency analysis of detectors in non-Gaussian noise, Johns Hopkins Conf. on Inf. Systems and Science, March, 1987, Baltimore, MD.
- Ian F. Blake, Data communications and security, IEEE Pacific Rim Conf. on Comm., Comp. and Signal Processing, June, 1987, Victoria, B.C..
- Klas Forsberg and Ian F. Blake, The enumeration of (d,k) sequences, Twenty Sixth Annual Allerton Conference on Communication, Control and Computing, Illinois, 1988.
- T.Y. Tong and Ian F. Blake, Diversity and coding in spread spectrum systems, Canadian Conference on Electrical and Computer Engineering, Vancouver, B.C. 1988.

- Ian F. Blake and Klas Forsberg, The enumeration of constrained sequences, International Conference on Computing and Information, '89, Hamilton, May, 1989.
- T.Y. Tong and Ian F. Blake, Diversity and coding for an interference model, MILCOM '89, Boston, Mass., October, 1989, pp. 29.1.1-29.1.5.
- Ian F. Blake and K. Kith, On the complete weight enumerator of Reed-Solomon codes, Conference on Information Systems and Sciences, Princeton, NJ, March, 1990.
- Q. Wang, V.K. Bhargava, T.A. Gulliver and I.F. Blake, Coding for frequency hopped spread spectrum satellite communications, Canadian Conference on Electrical and Computer Engineering, Ottawa, 1990.
- Q. Qang, T.A. Gulliver, L.L. Mason and I.F. Blake, Coding for slow frequency hopped differential phase shift keying, MILCOM '90, Monterey, California, September 30-October 3, 1990.
- Ian F. Blake, S. Gao and R.C. Mullin, Factorization of polynomials of the type $f(x^t)$, International Conference on Finite Fields, Coding Theory and Advances in Communications and Computing, Las Vegas, Nevada, August 7-10, 1991.
- S. Bross and Ian F. Blake, Trellis codes for the binary and N-user adder channel, Princeton Conference on Inf. Systems and Sciences, March, 1992.
- Z. Tan and Ian F. Blake, Multipath diversity reception of hybrid DS-SFH spread spectrum multiple access over Rician multipath fading channels, International Conf. on Selected Topics in Wireless Communications, Vancouver, B.C., June, 1992.
- T. Yaghoobian and Ian F. Blake, Codes from hyperelliptic curves, Thirtieth Annual Conference on Communications, Control and Computing, September, 1992.
- Z. Tan and Ian F. Blake, Performance analysis of non-coherent hybrid DS-SFH spread spectrum communications over Rayleigh multipath fading channels, MILCOM '92, San Diego, October, 1992.
- S. Bross and Ian F. Blake, Upper Bound for uniquely decodable codes in a binary input N-user adder channel, Intl. Symp. Info. Theory, Houston, Texas, January, 1993.
- T. Yaghoobian and Ian F. Blake, A new remainder based decoding algorithm for Reed-Solomon codes, Intl. Symp. Info. Theory, San Antonio, Texas, January, 1993.
- M. Alencar and Ian F. Blake, Analysis of the capacity region for the non-cooperative multiaccess channel with Rician fading, ICC '93, Geneva, Switzerland, May, 1993.
- M. Alencar and Ian F. Blake, Analysis of the capacity for a Markovian multiple access channel, IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, May, 1993.
- Ian F. Blake, S. Gao and R.C. Mullin, Specific irreducible polynomials with linearly independent roots over finite fields, Conference on Finite Fields, Las Vegas, August, 1993.
- Ian F. Blake, S. Gao and R. Lambert, Constructive problems for irreducible polynomials over finite fields, Plenary talk, Canadian Society for Information Theory workshop, Ottawa, June, 1993 (also in Lecture Notes in Computer Science, Vol. 793, 1-23, Springer-Verlag).
- Marcelo S. Alencar and Ian F. Blake, The capacity of a code division multiple access channel, ISCOM'93, Taiwan, December, 1993. (invited)
- Ian F. Blake, Reed-Solomon and Algebraic-Geometry Codes, ISCOM'93, 4-hour tutorial, Taiwan, December, 1993.
- Ian F. Blake, NSERC, Excellence and Electrical Engineering, Canadian Conference on Electrical Engineering, September, 1993 (plenary talk, invited).

- Marcelo S. Alencar and Ian F. Blake, A bound on the capacity of a CDMA system with DPSK modulation, ITS, Rio de Janeiro, Brazil, August, 1994.
- D. Dabiri and Ian F. Blake, On the module theoretic approach to the solution to congruences, 17th Biennial Symposium on Communications, Kingston, May, 1994.
- Ian F. Blake, Coding for the Binary Adder Channel, International Conference on Coding and Cryptography, February, 1994 in Coding and Cryptography, Kluwer Academic press, 1994.
- D. Dabiri and Ian F. Blake, Fast parallel algorithms for decoding Reed-Solomon codes, International Symposium on Information Theory, Trondheim, Norway, June, 1994.
- Ian F. Blake, Darius Dabiri and Tomik Yaghoobian, Decoding Reed-Solomon codes, Oberwolfach, Mathematisches Forschungsinstitut Oberwolfach, April, 1994 (invited).
- Darius Dabiri and Ian F. Blake, A system theoretic approach to decoding algebraic geometry codes, American Mathematical Society, Central Section Meeting, Chicago, Illinois, March, 1995 (invited).
- D. Dabiri and Ian F. Blake, Multilevel codes based on matrix completion, International Symposium on Information Theory, Whistler, B.C., September, 1995.
- V. Tarokh and Ian F. Blake, Trellis complexity versus the coding gain of lattices, International Symposium on Information Theory, Whistler, B.C., September, 1995.
- V. Tarokh and Ian F. Blake, On the label group complexity of lattices, Thirty-third Annual Allerton Conference on Communication, Control and Computing, October 4-6, 1995, 710-713.
- C. Pimentel and Ian F. Blake, Enumeration of Markov chains and error statistics for Gilbert-Elliott channels, Thirty-third Annual Allerton Conference on Communication, Control and Computing, October 4-6, 1995, 648-657.
- C. Pimentel and Ian F. Blake, Derivation of burst error statistics for finite state channel models using a combinatorial approach, 30th Annual Conference on Information Sciences and Systems, Princeton University, 20-22 March, 1996.
- C. Pimentel and Ian F. Blake, Modeling burst channels using finite state Markov models, 18th Biennial Symposium on Communications, Kingston, June, 1996.
- Ian F. Blake, Elliptic curve cryptography, ISITA'96, Victoria, B.C. 17-20 September, 1996 (invited talk).
- V. Tarokh and Ian F. Blake, Dense Mordell-Weil lattices of elliptic curves over function fields: explicit computation, Thirty-fourth Annual Allerton Conference on Communication, Control and Computing, October 2-4, 1996.
- A. Banihashemi and Ian F. Blake, Minimal trellis diagrams of lattices, ISIT'97, Ulm, Germany, June, 1997.
- A. Banihashemi and Ian F. Blake, New upper bounds on trellis complexity of lattices, ISIT'97, Ulm, Germany, June, 1997.
- A. Banihashemi and Ian F. Blake, New lower bounds on trellis complexity of lattices, Canadian Workshop on Information Theory, Toronto, Ont., June, 1997.
- A. H. Banihashemi and Ian F. Blake, On the trellis complexity of some important lattices, Information Theory Workshop, Svalbard, Norway, July, 1997.
- Cecilio Pimentel and Ian F. Blake, Non-interleaved Reed-Solomon coding performance on finite state channels, ICC'97, Montreal, Canada, June, 1997.

- Ian F. Blake, Ron M. Roth and Gadiel Seroussi, Implementation issues for elliptic curve cryptosystems over fields of characteristic two, Information Theory Workshop, Svalbard, Norway, July, 1997.
- H. Wu, M.A. Hasan and Ian F. Blake, Low complexity bit-parallel finite field multipliers, Proceedings of the 5th Canadian Workshop on Information Theory, pp. 109-112, 1997.
- Ian F. Blake, Curves with many points, Thirty-fifth Annual Allerton Conference on Communication, Control and Computing, September 29 October 1, 1997.
- Ian F. Blake, Public key cryptosystems, PKS'98, Toronto, Ontario, 19-22 April, 1998.
- Ian F. Blake, Point counting on elliptic curves, IMA Workshop on Coding and Cryptography, July, 1998, Minneapolis, MN.
- H. Wu, M.A. Hasan and Ian F. Blake, Efficient computation for multiple points for elliptic curve cryptosystems, ISIT'98, Boston, MA, August, 1998.
- Ian F. Blake, R.M. Roth and G. Seroussi, On the solution of an elliptic curve over a field of characteristic two, ISIT'98, Boston, MA, August, 1998.
- Huapeng Wu, M. Anwarul Hasan, and Ian F. Blake, Highly Regular Architectures for Finite Field Computation Using Redundant Basis, Workshop on Cryptographic Hardware and Embedded Systems, Worcester, MA, August 12-13, 1999.
- Ian F. Blake, Applications of curves with many points, AAECC, Hawaii, November, 1999, (Invited talk).
- Ian F. Blake, Lattices and cryptography, Forneyfest, MIT, March, 2000 (Invited talk).
- Ian F. Blake, Construction techniques for graphs with large girth and LDPC, 38th Allerton Conference, September, 2000 (invited talk).
- Ian F. Blake, The discrete logarithm problem revisited, Workshop on Coding and Cryptography, Institute of Mathematical Sciences, National University of Singapore, July-August, 2001 (invited paper).
- Ian F. Blake, Expander codes revisited, 39th Allerton Conference, September, 2002 (invited talk).
- Ian F. Blake, Theo Garefalakis and Kumar Murty, On two towers of function fields, 39th Allerton Conference, September, 2002.
- Ian F. Blake, Codes, graphs, expanders and girth, Joint Meeting of the AMS and MAA, San Diego, January, 2002 (invited talk).
- Ian F. Blake, Cryptographic protocols, IEEE Communications Society, Communication Theory Workshop, Florida, May, 2002 (invited talk and session organizer).
- Ian F. Blake, Distributed protocols for cryptography, 2002 Summer Meeting of the Canadian Mathematical Society (invited talk), Quebec City.
- M. Shamsi, Permutation space-time codes, Canadian Workshop on Information Theory, May 2003.
- J. Xu, S. Lin and Ian F. Blake, On products of graphs for LDPC codes, IEEE Workshop on Information Theory, Paris, April, 2003.
- Huapeng Wu, M. Anwar Hasan and Ian F. Blake, Speeding up RSA and elliptic curve systems by choosing suitable moduli, CCC, September 2003.
- Mehrdad Shamsi and Ian F. Blake, Space-time codes with triangular core, ICC, Communication Theory Symposium, Paris, June 2004.
- E.C. Park and Ian F. Blake, Recursive expressions for tree-based key distribution schemes, Conference on Information and System Science, Princeton University, March 2004.

- Mehrdad Shamsi and Ian F. Blake, Space-time codes from property L, IEEE ISIT 2004, Chicago, June 2004.
- K.W. Shum, Ian F. Blake and K. Murty, On the zeta functions of two towers of function fields, IEEE ISIT 2004, Chicago, June 2004.
- Ian F. Blake, Bao Li and Guangwu Xu, Protocols for sharing a product, Algebraic Methods in Cryptography, China, July, 2005.
- Ian F. Blake and Vlad Kolesnikov, Strong conditional oblivious transfer and computing on intervals, *Asiacrypt 2004*, Lecture Notes in Computer Science, Vol. 3329, pp. 119-134, 2004.
- Mehrdad Shamsi, Masoud Ardakani and Ian F. Blake, A new modulation scheme for space-time codes, accepted, Seoul, Korea, May 2005.
- Aldar C-F. Chan and Ian F. Blake, Scalable, server-passive, user-anonymous timed release cryptography, ICDCS 2005, Ohio, June 2005. (75 papers accepted out of 540 submitted.)
- Ian F. Blake and V. Kolesnikov, Conditional encrypted mapping and comparing encrypted numbers, *Financial Cryptography and Data Security 2006*, LNCS v. 4107, pp. 206-220, February 2006.
- Ian F. Blake and E.C. Park, Coding for private information retrieval, 8th International Symposium on Communication Theory and Applications, 17-22 July, 2005, Ambleside, UK.
- C. Studholme and Ian F. Blake, Windowed erasure codes, ISIT 2006, Seattle, 9-16 July, 2006.
- E.C. Park and Ian F. Blake, Reducing Communication Overhead for Sensor Network Key Pre-distribution Schemes, to First International Workshop on Distributed Sensor Systems, Hawaii, August, 2007.
- Ian F. Blake and Theo Garofalakis, A note on Kloosterman sums, ITA Conference, UCSD, February, 2008.
- Ian F. Blake, Aspects of identity based encryption, Workshop on Foundations of wireless networks and beyond, Maryland, October, 2008.
- Ian F. Blake, Coding for erasures and random matrices, ISCTA 2009, Ambleside, UK, July, 2009.
- Ehsan Vahedi, Vahid Shah-Mansouri, Vincent W.S. Wong, and Ian F. Blake, A Probabilistic Approach for Detecting Blocking Attack in RFID Systems, accepted ICC 2010, Cape Town, South Africa, 23 - 27 May, 2010.
- Ian F. Blake, Abelian varieties in coding and cryptography, ITW 2010, Aug. 30 - Sept. 3, 2010, Dublin.

Dongning Guo

Biography

Dongning Guo received the B.Eng. degree from the University of Science & Technology of China, the M.Eng. degree from the National University of Singapore, and the M.A. and Ph.D. degrees from Princeton University, Princeton, NJ. He was an R&D Engineer in the Center for Wireless Communications (now the Institute for Infocom Research), Singapore, from 1998 to 1999. He joined the the Department of Electrical Engineering and Computer Science at Northwestern University, Evanston, IL, in 2004, where he is currently an Associate Professor. He was a Visiting Professor at Norwegian University of Science and Technology in summer 2006. His research interests are in information theory, communications, and networking. He received the Huber & Suhner Best Student Paper Award in the International Zurich Seminar on Broadband Communications in 2000 and the IEEE Marconi Prize Paper Award in Wireless Communications in 2010. He is also a recipient of the National Science Foundation Faculty Early Career Development (CAREER) Award in 2007.

Publications

Book Chapters

- [B1] D. Guo and T. Tanaka, “Generic multiuser detection and statistical physics,” in *Advances in Multiuser Detection* (M. Honig, ed.), ch. 5, Wiley-IEEE Press, 2009.
- [B2] D. Guo and S. Verdú, “Multiuser detection and statistical mechanics,” in *Communications, Information and Network Security* (V. Bhargava, H. V. Poor, V. Tarokh, and S. Yoon, eds.), ch. 13, pp. 229–277, Kluwer Academic Publishers, 2002.

Journal Articles (Published)

- [J1] D. Guo, Y. Wu, S. Shamai, and S. Verdú, “Estimation in Gaussian noise: Properties of the minimum mean-square error,” *IEEE Trans. Inform. Theory*, 2011. To appear.
- [J2] M. Agarwal, D. Guo, and M. L. Honig, “Limited-rate channel state feedback for multicarrier block fading channels,” *IEEE Trans. Inform. Theory*, Dec. 2010. In press.
- [J3] N. Merhav, D. Guo, and S. Shamai, “Statistical physics of signal estimation in Gaussian noise: Theory and examples of phase transition,” *IEEE Trans. Inform. Theory*, vol. 56, pp. 1400–1416, Mar. 2010.
- [J4] Y. Zhu, D. Guo, and M. L. Honig, “A message-passing approach to joint channel estimation, interference mitigation and decoding,” *IEEE Trans. Wireless Commun.*, vol. 8, pp. 6008–6018, Dec. 2009.
- [J5] J. Luo and D. Guo, “On the entropy rate of hidden Markov processes observed through arbitrary memoryless channels,” *IEEE Trans. Inform. Theory*, vol. 55, pp. 1460–1467, Apr. 2009.
- [J6] D. J. Ryan, I. V. L. Clarkson, I. B. Collings, D. Guo, and M. L. Honig, “QAM and PSK codebooks for limited feedback MIMO beamforming,” *IEEE Trans. Commun.*, vol. 57, pp. 1184–1196, Apr. 2009.
- [J7] J. Andrews, N. Jindal, M. Haenggi, R. Berry, S. Jafar, D. Guo, S. Shakkottai, R. Heath Jr, M. Neely, S. Weber, A. Yener, and P. Stone, “Rethinking information theory for mobile ad hoc networks,” *IEEE Communication Magazine*, vol. 46, pp. 94–101, Dec. 2008.
- [J8] D. Guo, S. Shamai (Shitz), and S. Verdú, “Mutual information and conditional mean estimation in Poisson channels,” *IEEE Trans. Inform. Theory*, vol. 54, pp. 1837–1849, May 2008.
- [J9] D. Guo and C.-C. Wang, “Multiuser detection of sparsely spread CDMA,” *IEEE J. Select. Areas Commun.*, vol. 26, pp. 421–431, Apr. 2008.
- [J10] R. R. Müller, D. Guo, and A. Moustakas, “Vector precoding for wireless MIMO systems and its replica analysis,” *IEEE J. Select. Areas Commun.*, vol. 26, pp. 530–540, Apr. 2008.
- [J11] F. Meshkati, D. Guo, H. V. Poor, and S. C. Schwartz, “A unified approach to energy-efficient power control in large CDMA systems,” *IEEE Trans. Wireless Commun.*, vol. 7, pp. 1208–1216, Apr. 2008.
- [J12] D. Guo, “Some large linear systems in communications: Estimation, information and statistical physics,” *Journal of Physics: Conference Series*, vol. 95, p. 012007, Jan. 2008.

- [J13] R. R. Müller, D. Guo, and A. Moustakas, “A quadratic programming problem arising from vector precoding in wireless communications,” *Journal of Physics: Conference Series*, vol. 95, p. 012006, Jan. 2008.
- [J14] S. Verdú and D. Guo, “A simple proof of the entropy power inequality,” *IEEE Trans. Inform. Theory*, pp. 2165–2166, May 2006.
- [J15] D. Guo, “Performance of multicarrier CDMA in frequency-selective fading via statistical physics,” *IEEE Trans. Inform. Theory*, vol. 52, pp. 1765–1774, Apr. 2006.
- [J16] D. Guo, S. Shamai (Shitz), and S. Verdú, “Mutual information and minimum mean-square error in Gaussian channels,” *IEEE Trans. Inform. Theory*, vol. 51, pp. 1261–1282, Apr. 2005.
- [J17] D. Guo and S. Verdú, “Randomly spread CDMA: Asymptotics via statistical physics,” *IEEE Trans. Inform. Theory*, vol. 51, pp. 1982–2010, June 2005.
- [J18] D. Guo, S. Verdú, and L. K. Rasmussen, “Asymptotic normality of linear multiuser receiver outputs,” *IEEE Trans. Inform. Theory*, vol. 48, pp. 3080–3095, Dec. 2002.
- [J19] D. Guo, L. K. Rasmussen, S. Sun, and T. J. Lim, “A matrix-algebraic approach to linear parallel interference cancellation in CDMA,” *IEEE Trans. Commun.*, vol. 48, pp. 152–161, Jan. 2000.
- [J20] D. Guo, L. K. Rasmussen, and T. J. Lim, “Linear parallel interference cancellation in long-code CDMA multiuser detection,” *IEEE J. Select. Areas Commun.*, vol. 17, pp. 2074–2081, Dec. 1999.

Journal Articles (Under Review/In Preparation)

- [JR1] H. Zhou, P. Fan, and D. Guo, “Joint channel probing and proportional fair scheduling in wireless networks,” *Submitted to IEEE Trans. Wireless Commun.*, 2010.
- [JR2] Y. Zhu and D. Guo, “Ergodic fading Z-interference channels without state information at transmitters,” *submitted to IEEE Trans. Inform. Theory*, 2010. Revised.
- [JR3] K. Huang, J. G. Andrews, R. W. Heath Jr., D. Guo, and R. A. Berry, “Spatial interference cancelation for multi-antenna mobile ad hoc networks,” *submitted to IEEE Trans. Inform. Theory*, 2010. Revised. <http://arxiv.org/abs/0807.1773>.

Conference Papers (Submitted and Published)

- [C1] H. Zhou, P. Fan, and D. Guo, “The impact of limited information on proportional fair scheduling in wireless networks,” in *Proc. IEEE GLOBECOM*, Miami, FL, USA, 2010. To be presented.
- [C2] M. Xu, D. Guo, and M. L. Honig, “Two-cell downlink noncoherent cooperation without transmitter phase alignment,” in *Proc. IEEE GLOBECOM*, Miami, FL, USA, 2010. To be presented.
- [C3] D. Guo and L. Zhang, “Rapid on-off-division duplex for mobile ad hoc networks,” in *Proc. Allerton Conf. Commun., Control, & Computing*, Monticello, IL, USA, 2010.
- [C4] K. H. Hui, D. Guo, and R. A. Berry, “Medium access control via nearest neighbor interactions for regular wireless networks,” in *Proc. IEEE Int. Symp. Inform. Theory*, Austin, TX, USA, 2010.

- [C5] Y. Zhu and D. Guo, "On the capacity region of fading one-sided interference channels without CSIT," in *Proc. IEEE Int. Symp. Inform. Theory*, Austin, TX, USA, 2010.
- [C6] K.-H. Hui, Y. E. Sagduyu, D. Guo, and R. A. Berry, "The maximum stable broadcast throughput for wireless line networks with network coding and topology control," in *Proc. Conf. Inform. Sciences & Systems*, Princeton, NJ, USA, 2010.
- [C7] Y. Zhu and D. Guo, "Capacity region of layered erasure one-sided interference channels without CSIT," in *Proc. IEEE Inform. Theory Workshop*, Cairo, Egypt, 2010.
- [C8] M. Xu, D. Guo, and M. L. Honig, "MIMO precoding with limited rate feedback: Simple quantizers work well," in *Proc. IEEE GLOBECOM*, Hawaii, USA, 2009.
- [C9] F. Rubio, D. Guo, M. L. Honig, and X. Mestre, "Asymptotic diversity analysis of MIMO systems with limited training," in *Proc. International Workshop on Random Matrix Theory for Wireless Communications (RMTfWC)*, St.-Petersburg, Russia, 2009.
- [C10] Y. Zhu and D. Guo, "Isotropic MIMO interference channels without CSIT: The loss of degrees of freedom," in *Proc. Allerton Conf. Commun., Control, & Computing*, Monticello, IL, USA, Oct. 2009.
- [C11] J. Luo and D. Guo, "Compressed neighbor discovery for wireless ad hoc networks: the Rayleigh fading case," in *Proc. Allerton Conf. Commun., Control, & Computing*, Monticello, IL, USA, Oct. 2009.
- [C12] K. H. Hui, D. Guo, R. A. Berry, and M. Haenggi, "Performance analysis of MAC protocols in wireless line networks using statistical mechanics," in *Proc. Allerton Conf. Commun., Control, & Computing*, Monticello, IL, USA, Oct. 2009.
- [C13] D. Guo, D. Baron, and S. Shamai (Shitz), "A single-letter characterization of optimal noisy compressed sensing," in *Proc. Allerton Conf. Commun., Control, & Computing*, Monticello, IL, USA, Oct. 2009.
- [C14] D. Guo, "Relative entropy and score function: New information-estimation relationships through arbitrary additive perturbation," in *Proc. IEEE Int. Symp. Inform. Theory*, Seoul, Korea, 2009.
- [C15] M. Xu, D. Guo, and M. L. Honig, "Limited feedback for multi-carrier beamforming: A rate-distortion approach," in *Proc. IEEE Int. Symp. Inform. Theory*, Seoul, Korea, 2009.
- [C16] M. Agarwal, D. Guo, and M. L. Honig, "Limited feedback for multicarrier block fading channels: A rate distortion approach," in *Proc. IEEE Inform. Theory Workshop*, Volos, Greece, 2009.
- [C17] K. Huang, J. G. Andrews, R. W. Heath Jr., D. Guo, and R. A. Berry, "Spatial interference cancelation for mobile ad hoc networks: Perfect CSI," in *Proc. IEEE GLOBECOM, Ad Hoc, Sensor and Mesh Networking Symposium*, New Orleans, LA, USA, 2008.
- [C18] Y. E. Sagduyu, D. Guo, and R. Berry, "Throughput and stability of digital and analog network coding for wireless networks with single and multiple relays," in *International Wireless Internet Conference (WICON)*, Maui, Hawaii, USA, 2008. (invited).

- [C19] K. Huang, J. G. Andrews, R. W. Heath Jr., D. Guo, and R. A. Berry, "Spatial interference cancelation for mobile ad hoc networks: Imperfect CSI," in *Asilomar Conference*, Pacific Grove, CA, USA, 2008.
- [C20] J. Luo and D. Guo, "Neighbor discovery in wireless ad hoc networks based on group testing," in *Proc. Allerton Conf. Commun., Control, & Computing*, Monticello, IL, USA, 2008.
- [C21] D. Guo, Y. Zhu, and M. L. Honig, "Co-channel interference mitigation in multiuser systems with unknown channels," in *Proc. XXIXth URSI General Assembly*, Chicago, IL, USA, Aug. 2008. (invited).
- [C22] M. Agarwal, D. Guo, and M. L. Honig, "Channel and receiver state feedback for frequency-selective block fading channel," in *Proc. IEEE Int. Symp. Inform. Theory*, Toronto, Canada, July 2008.
- [C23] D. Guo, S. Shamai, and S. Verdú, "Estimation of non-Gaussian random variables in Gaussian noise: Properties of the MMSE," in *Proc. IEEE Int. Symp. Inform. Theory*, Toronto, Canada, 2008.
- [C24] Y. E. Sagduyu, D. Guo, and R. A. Berry, "Throughput optimal control for relay-assisted wireless broadcast with network coding," in *IEEE International Workshop on Wireless Network Coding (WiNC)*, San Francisco, CA, USA, 2008.
- [C25] Y. Zhu, D. Guo, and M. L. Honig, "Joint channel estimation and interference mitigation in wireless networks using belief propagation," in *Proc. IEEE Int. Conf. Commun.*, Beijing, China, May 2008.
- [C26] M. Agarwal, D. Guo, and M. L. Honig, "Multi-carrier transmission with limited feedback: Power loading over sub-channel groups," in *Proc. IEEE Int. Conf. Commun.*, pp. 981–985, Beijing, China, 2008.
- [C27] Y. E. Sagduyu, D. Guo, and R. A. Berry, "On the delay and throughput of digital and analog network coding for wireless broadcast," in *Proc. Conf. Inform. Sciences & Systems*, Princeton, NJ, USA, 2008.
- [C28] J. Luo and D. Guo, "On the entropy and filtering of hidden Markov processes observed via arbitrary channels," in *Proc. Conf. Inform. Sciences & Systems*, Princeton, NJ, USA, 2008.
- [C29] F. Rubio, D. Guo, M. L. Honig, and X. Mestre, "On optimal training and beamforming in uncorrelated MIMO systems with feedback," in *Proc. Conf. Inform. Sciences & Systems*, Princeton, NJ, USA, 2008.
- [C30] R. R. Müller, D. Guo, and A. Moustakas, "Vector precoding in high dimensions: A replica analysis," in *Proc. IEEE Int. Symp. Inform. Theory*, Nice, France, June 2007.
- [C31] R. R. Müller, D. Guo, and A. Moustakas, "Vector precoding in wireless communications: A replica symmetric analysis," in *Proc. Second International Conference on Performance Evaluation Methodologies and Tools*, Nantes, France, Oct. 2007.
- [C32] D. Guo and C.-C. Wang, "Random sparse linear systems observed via arbitrary channels: A decoupling principle," in *Proc. IEEE Int. Symp. Inform. Theory*, Nice, France, June 2007.
- [C33] M. Agarwal, D. Guo, and M. L. Honig, "Error exponent for AWGN channel with partial sequential feedback," in *Proc. IEEE Int. Symp. Inform. Theory*, Nice, France, June 2007.

- [C34] D. J. Ryan, I. V. L. Clarkson, I. B. Collings, D. Guo, and M. Honig, "QAM codebooks for low-complexity limited feedback MIMO beamforming," in *Proc. IEEE Int. Conf. Commun.*, Glasgow, Scotland, June 2007.
- [C35] K. Sil, M. Agarwal, D. Guo, M. Honig, and W. Santipach, "Performance of Turbo decision-feedback detection and decoding in downlink OFDM," in *Proc. IEEE Wireless Commun. & Networking Conf.*, Hong Kong, China, Mar. 2007.
- [C36] C.-C. Wang and D. Guo, "Belief propagation is asymptotically equivalent to MAP detection for sparse linear systems," in *Proc. Allerton Conf. Commun., Control, & Computing*, pp. 926–935, Monticello, IL, USA, Oct. 2006.
- [C37] D. Guo and C.-C. Wang, "Asymptotic mean-square optimality of belief propagation for sparse linear systems," in *Proc. IEEE Inform. Theory Workshop*, Chengdu, China, Oct. 2006.
- [C38] D. Guo, S. Shamai, and S. Verdú, "Proof of entropy power inequalities via MMSE," in *Proc. IEEE Int. Symp. Inform. Theory*, pp. 1011–1015, Seattle, WA, USA, July 2006.
- [C39] D. Guo, "Error performance of multicarrier CDMA infrequency-selective fading," in *Proc. IEEE Globecom*, St. Louis, MI USA, Nov.–Dec. 2005.
- [C40] F. Meshkati, H. V. Poor, S. C. Schwartz, and D. Guo, "A unified power control algorithm for multiuser detectors in large systems: Convergence and performance," in *Proc. Allerton Conf. Commun., Control, & Computing*, Monticello, IL, USA, Oct. 2005.
- [C41] D. Guo, "Performance of multicarrier and multirate CDMA: A decoupling result," in *Proc. Allerton Conf. Commun., Control, & Computing*, Monticello, IL, USA, Oct. 2005.
- [C42] D. Guo, "Performance of synchronous multirate CDMA via statistical physics," in *Proc. IEEE Int. Symp. Information Theory*, Adelaide, Australia, Sept. 2005.
- [C43] D. Guo, S. Shamai, and S. Verdú, "Additive non-Gaussian noise channels: Mutual information and conditional mean estimation," in *Proc. IEEE Int. Symp. Inform. Theory*, Adelaide, Australia, Sept. 2005.
- [C44] D. Guo, S. Shamai, and S. Verdú, "Mutual information and conditional mean estimation in Poisson channels," in *Proc. IEEE Inform. Theory Workshop*, pp. 265–270, San Antonio, TX, USA, 2004.
- [C45] D. Guo, S. Shamai, and S. Verdú, "Mutual information and MMSE in Gaussian channels," in *Proc. IEEE Int. Symp. Information Theory*, p. 347, Chicago, IL, USA, 2004.
- [C46] F. Meshkati, D. Guo, H. V. Poor, S. Schwartz, and N. B. Mandayam, "A unified approach to power control for multiuser detectors," in *Proc. 2nd International Workshop on Signal Processing for Wireless Communications*, London, England, 2004.
- [C47] D. Guo and S. Verdú, "Decoupling of CDMA multiuser detection via the replica method," in *Proc. Allerton Conf. Commun., Control, & Computing*, Monticello, IL, USA, 2003. (Invited).
- [C48] D. Guo and S. Verdú, "Replica analysis of CDMA spectral efficiency," in *Proc. IEEE Inform. Theory Workshop*, Paris, France, 2003. (Invited).

- [C49] D. Guo and S. Verdú, "Spectral efficiency of large-system CDMA via statistical physics," in *Proc. Conf. Inform. Sciences & Systems*, Baltimore, MD, USA, 2003.
- [C50] D. Guo and S. Verdú, "Minimum probability of error of many-user CDMA without power control," in *Proc. IEEE Int. Symp. Information Theory*, p. 188, Lausanne, Switzerland, 2002.
- [C51] D. Guo, S. Verdú, and L. K. Rasmussen, "Asymptotic normality of linear CDMA multiuser detection outputs," in *Proc. IEEE Int. Symp. Information Theory*, p. 307, Washington, D.C., 2001.
- [C52] K. V. Ravi, D. Guo, and K. L. Cheah, "Performance evaluation of an OFDM-based LMDS using measured channel models," in *Proc. IEEE Wireless Commun. Networking Conf.*, vol. 3, pp. 1511–1515, Chicago, IL, USA, 2000.
- [C53] D. Guo and L. K. Rasmussen, "Linear parallel interference cancellation using fixed weighting factors for long-code CDMA," in *Proc. IEEE Int. Symp. Information Theory*, p. 332, Sorrento, Italy, 2000.
- [C54] D. Guo and L. K. Rasmussen, "MMSE-based parallel interference cancellation for long-code CDMA," in *Proc. Annual Zurich Seminar Broadband Commun.*, Zurich, Switzerland, 2000.
- [C55] K. L. Cheah, D. Guo, K. V. Ravi, and T. J. Lim, "Performance evaluation of LMDS with adaptive LMS equalisation," in *Proc. IEEE Asia-Pac. Conf. Comms. (ICCS)*, Singapore, 1999.
- [C56] T. J. Lim, D. Guo, and L. K. Rasmussen, "Noise enhancement in the family of decorrelating detectors for multiuser CDMA," in *Proceedings IEEE Asia-Pac. Conf. Comms./Int'l Conf. Comm. Systems (APCC/ICCS)*, pp. 401–405, Singapore, 1998.
- [C57] D. Guo, L. K. Rasmussen, S. Sun, T. J. Lim, and C. Cheah, "MMSE-based linear parallel interference cancellation in CDMA," in *Proceedings IEEE Fifth International Symposium on Spread Spectrum Techniques and Applications*, vol. 3, pp. 917–921, Sun City, South Africa, 1998.
- [C58] L. K. Rasmussen, D. Guo, T. J. Lim, and Y. Ma, "Aspects on linear parallel interference cancellation in CDMA," in *Proc. IEEE Int. Symp. Information Theory*, p. 37, MIT, Cambridge, MA USA, 1998.

September 17, 2010

Venkatesan Guruswami

Venkatesan Guruswami is an Associate Professor in the Computer Science Department at Carnegie Mellon University. Dr. Guruswami received his Bachelor's degree from the Indian Institute of Technology at Madras in 1997 and his Ph.D. from the Massachusetts Institute of Technology in 2001. From 2002-09, he was a faculty member in the Department of Computer Science and Engineering at the University of Washington. He was a Miller Research Fellow at the University of California, Berkeley during 2001-02, and a member in the School of Mathematics, Institute for Advanced Study during 2007-08.

Dr. Guruswami's research interests span several topics such as the theory of error-correcting codes, approximation algorithms and hardness of approximation results for optimization problems, pseudorandomness and combinatorics, computational complexity theory, and algebraic algorithms. Dr. Guruswami is a recipient of a Packard Fellowship (2005), Sloan Fellowship (2005), NSF Career award (2004), ACM's Doctoral Dissertation Award (2002), and the IEEE Information Theory Society Paper Award (2000).

List of Publications

VENKATESAN GURUSWAMI

September 2010

Books

- [B1] V. Guruswami. *Algorithmic Results in List Decoding*, volume 2 of *Foundations and Trends in Theoretical Computer Science (FnT-TCS)*. NOW publishers, January 2007.
- [B2] V. Guruswami. *List decoding of error-correcting codes*. Springer, Lecture Notes in Computer Science 3282, 2004. (Winning Thesis of the 2002 ACM Doctoral Dissertation Competition).

Refereed Journal Publications

Accepted papers

- [J1] V. Guruswami and A. Rudra. Soft decoding, dual BCH codes, and better list-decodable ϵ -biased codes. *IEEE Transactions on Information Theory*, 2010. Koetterfest special issue. Accepted for publication.
- [J2] V. Guruswami, J. Håstad, and S. Kopparty. On the list-decodability of random linear codes. *IEEE Transactions on Information Theory*, 2010. Koetterfest special issue. Accepted for publication.
- [J3] V. Guruswami and S. Vadhan. A lower bound on list size for list decoding. *IEEE Transactions on Information Theory*, November 2010. To appear.
- [J4] M. Andrews, J. Chuzhoy, V. Guruswami, S. Khanna, K. Talwar, and L. Zhang. Inapproximability of edge-disjoint paths and low congestion routing on undirected graphs. *Combinatorica*, 2010. Accepted for publication.

Published papers

- [J5] V. Guruswami and A. Rudra. The existence of concatenated codes list-decodable up to the Hamming bound. *IEEE Transactions on Information Theory*, 56(10):5195–5206, October 2010.
- [J6] V. Guruswami. Cyclotomic function fields, Artin-Frobenius automorphisms, and list error-correction with optimal rate. *Algebra and Number Theory*, 4(4):433–463, 2010.
- [J7] E. Ben-Sasson, V. Guruswami, T. Kaufman, M. Sudan, and M. Viderman. Locally testable codes require redundant testers. *SIAM Journal on Computing*, 39(7):3230–3247, 2010.
- [J8] V. Guruswami, J. Lee, and A. Razborov. Almost Euclidean sections of ℓ_1^n via expander codes. *Combinatorica*, 30(1):47–68, 2010.
- [J9] P. Gopalan and V. Guruswami. Hardness amplification within NP against deterministic algorithms. *Journal of Computer and System Sciences*, June 2010. Published online, Article in Press.
- [J10] V. Guruswami and P. Raghavendra. Hardness of solving sparse overdetermined linear systems: A 3-query PCP over integers. *ACM Transactions on Computation Theory*, 1(2), September 2009.
- [J11] V. Guruswami and P. Raghavendra. Hardness of learning halfspaces with noise. *SIAM Journal on Computing*, 39(2):742–765, 2009.
- [J12] V. Guruswami, C. Umans, and S. Vadhan. Unbalanced expanders and randomness extractors from Parvaresh-Vardy codes. *Journal of the ACM*, 56(4), 2009.
- [J13] V. Guruswami and A. Rudra. Error-correction up to the information-theoretic limit. *Communications of the ACM*, 52(3):87–95, March 2009. Invited Research Highlight.
- [J14] V. Guruswami and A. Rudra. Better binary list-decodable codes via multilevel concatenation. *IEEE Transactions on Information Theory*, 55(1):19–26, January 2009.
- [J15] V. Guruswami and V. Kabanets. Hardness amplification via space-efficient direct products. *Computational Complexity*, 17(4):475–500, December 2008.
- [J16] V. Guruswami and A. Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Transactions on Information Theory*, 54(1):135–150, January 2008.
- [J17] V. Guruswami and A. Patthak. Correlated Algebraic-Geometric codes: Improved list decoding over bounded alphabets. *Mathematics of Computation*, 77(261):447–473, January 2008.

- [J18] P. Gopalan, V. Guruswami, and R. Lipton. Algorithms for modular counting of roots of multivariate polynomials. *Algorithmica*, 50(4):479–496, 2008.
- [J19] N. Alon, V. Guruswami, T. Kaufman, and M. Sudan. Guessing secrets efficiently via list decoding. *ACM Transactions on Algorithms*, 3(4):Article No. 42, November 2007.
- [J20] I. Giotis and V. Guruswami. Correlation clustering with a fixed number of clusters. *Theory of Computing*, 2(13):249–266, 2006.
- [J21] V. Guruswami and A. Rudra. Limits to list decoding Reed-Solomon codes. *IEEE Transactions on Information Theory*, 52(8):3642–3649, August 2006.
- [J22] V. Guruswami and P. Indyk. Linear-time encodable/decodable codes with near-optimal rate. *IEEE Transactions on Information Theory*, 51(10):3393–3400, October 2005.
- [J23] M. Charikar, V. Guruswami, and A. Wirth. Clustering with qualitative information. *Journal of Computer and System Sciences*, 71(3):360–383, October 2005. Special issue: Learning Theory 2003.
- [J24] V. Guruswami and A. Vardy. Maximum-Likelihood Decoding of Reed-Solomon codes is NP-hard. *IEEE Transactions on Information Theory*, 51(7):2249–2256, July 2005.
- [J25] V. Guruswami, D. Micciancio, and O. Regev. The complexity of the covering radius problem. *Computational Complexity*, 14(2):90–121, June 2005. Special issue devoted to selected papers from the 2004 Conference on Computational Complexity (CCC’04).
- [J26] I. Dinur, V. Guruswami, S. Khot, and O. Regev. A new multilayered PCP and the hardness of hypergraph vertex cover. *SIAM Journal on Computing*, 34(5):1129–1146, 2005.
- [J27] V. Guruswami and S. Khanna. On the hardness of 4-coloring a 3-colorable graph. *SIAM Journal on Discrete Mathematics*, 18(1):30–40, 2004.
- [J28] L. Engebretsen and V. Guruswami. Is constraint satisfaction over two variables always easy? *Random Structures and Algorithms*, 25(2):150–178, September 2004.
- [J29] M. Guruswamy, V. Guruswami, and C. S. R. Murthy. Randomized routing and wavelength requirements in wavelength routed WDM multistage, hypercube, and de bruijn networks. *Journal of Parallel and Distributed Computing*, 64:385–399, 2004.
- [J30] V. Guruswami. List decoding from erasures: Bounds and code constructions. *IEEE Transactions on Information Theory*, 49(11):2826–2833, 2003.
- [J31] V. Guruswami. Inapproximability results for set splitting and satisfiability problems with no mixed clauses. *Algorithmica*, 38(3):451–469, December 2003.

- [J32] V. Guruswami, S. Khanna, R. Rajaraman, F. B. Shepherd, and M. Yannakakis. Near-optimal hardness results and approximation algorithms for edge-disjoint paths and related problems. *J. Comput. Syst. Sci.*, 67(3):473–496, 2003.
- [J33] V. Guruswami. Constructions of codes from number fields. *IEEE Transactions on Information Theory*, 49(3):594–603, 2003.
- [J34] V. Guruswami, J. Håstad, and M. Sudan. Hardness of approximate hypergraph coloring. *SIAM Journal on Computing*, 31(6):1663–1686, 2002.
- [J35] M. Charikar, R. Fagin, V. Guruswami, J. M. Kleinberg, P. Raghavan, and A. Sahai. Query strategies for priced information. *J. Comput. Syst. Sci.*, 64(4):785–819, 2002.
- [J36] V. Guruswami, C. P. Rangan, M. Chang, G. J. Chang, and C. K. Wong. The K_r -packing problem. *Computing*, 66(1):79–89, 2001.
- [J37] V. Guruswami, J. Håstad, M. Sudan, and D. Zuckerman. Combinatorial bounds for list decoding. *IEEE Transactions on Information Theory*, 48(5):1021–1035, 2002.
- [J38] V. Guruswami and M. Sudan. On representations of Algebraic-geometric codes for list decoding. *IEEE Transactions on Information Theory*, 47(4):1610–1613, 2001.
- [J39] V. Guruswami and C. P. Rangan. Algorithmic aspects of clique-transversal and clique-independent sets. *Discrete Applied Mathematics*, 100(3):183–202, 2000.
- [J40] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and Algebraic-geometric codes. *IEEE Transactions on Information Theory*, 45(6):1757–1767, 1999.
- [J41] V. Guruswami. Enumerative aspects of certain classes of perfect graphs. *Discrete Mathematics*, 205:97–117, 1999.
- [J42] V. Guruswami. Maximum cut on line and total graphs. *Discrete Applied Mathematics*, 92:217–221, 1999.
- [J43] V. Guruswami and C. P. Rangan. A natural family of optimization problems with arbitrarily small approximation thresholds. *Information Processing Letters*, 68(5):241–248, 1998.
- [J44] V. Guruswami, U. Rotics, M. S. Madanlal, J. Makowsky, and C. P. Rangan. Restrictions of minimum spanner problems. *Information and Computation*, 136(2):143–164, 1997.
- [J45] M. S. Madanlal, V. Guruswami, and C. P. Rangan. Tree 3-spanners on interval, permutation, and regular bipartite graphs. *Information Processing Letters*, 59:97–102, 1996.

Papers in refereed conferences

- [C1] V. Guruswami and Y. Zhou. Tight bounds on the approximability of almost-satisfiable Horn-Sat and exact hitting set. In *Proceedings of the 22nd Annual ACM-SIAM Symposium on Discrete Algorithms*, January 2011. To appear.
- [C2] V. Guruswami and A. K. Sinop. The complexity of finding independent sets in bounded degree (hyper)graphs of low chromatic number. In *Proceedings of the 22nd Annual ACM-SIAM Symposium on Discrete Algorithms*, January 2011. To appear.
- [C3] V. Guruswami and A. Smith. Codes for computationally simple channels: Explicit codes with optimal rate. In *Proceedings of the 51st IEEE Symposium on the Foundations of Computer Science*, October 2010. To appear.
- [C4] V. Guruswami, J. Håstad, and S. Kopparty. On the list-decodability of random linear codes. In *Proceedings of the 42th ACM Symposium on Theory of Computing*, pages 409–416, June 2010.
- [C5] V. Guruswami and R. Saket. On the inapproximability of vertex cover on k -partite k -uniform hypergraphs. In *Proceedings of the 37th International Colloquium on Automata, Languages and Programming*, pages 360–371, 2010.
- [C6] V. Guruswami, S. Khot, R. O’Donnell, P. Papat, M. Tulsiani, and Y. Wu. SDP gaps for 2-to-1 and other Label-Cover variants. In *Proceedings of the 37th International Colloquium on Automata, Languages and Programming*, pages 617–628, 2010.
- [C7] V. Feldman, V. Guruswami, P. Raghavendra, and Y. Wu. Agnostic learning of monomials by halfspaces is hard. In *Proceedings of the 50th IEEE Symposium on Foundations of Computer Science*, pages 385–394, October 2009.
- [C8] V. Guruswami and A. K. Sinop. Improved inapproximability results for maximum k -colorable subgraph. In *Proceedings of the 12th International Workshop on Approximation, Randomization, and Combinatorial Optimization: Algorithms and Techniques (APPROX)*, pages 163–176, 2009.
- [C9] M. Charikar, V. Guruswami, and R. Manokaran. Every permutation CSP of arity 3 is approximation resistant. In *Proceedings of the 24th IEEE Conference on Computational Complexity*, pages 62–73, July 2009.
- [C10] E. Ben-Sasson, V. Guruswami, T. Kaufman, M. Sudan, and M. Viderman. Locally testable codes require redundant testers. In *Proceedings of the 24th IEEE Conference on Computational Complexity*, pages 52–61, July 2009.
- [C11] V. Guruswami. Artin automorphisms, cyclotomic function fields, and folded list-decodable codes. In *Proceedings of the 41st ACM Symposium on Theory of Computing (STOC)*, pages 23–32, May-June 2009.

- [C12] P. Gopalan, V. Guruswami, and P. Raghavendra. List decoding tensor products and interleaved codes. In *Proceedings of the 41st ACM Symposium on Theory of Computing (STOC)*, pages 13–22, May-June 2009.
- [C13] M. H. Bateni, M. Charikar, and V. Guruswami. Maxmin allocation via degree lower-bounded arborescences. In *Proceedings of the 41st ACM Symposium on Theory of Computing (STOC)*, pages 543–552, May-June 2009.
- [C14] V. Guruswami, R. Manokaran, and P. Raghavendra. Beating the random ordering is hard: Inapproximability of maximum acyclic subgraph. In *Proceedings of the 49th IEEE Symposium on Foundations of Computer Science*, pages 573–582, October 2008.
- [C15] V. Guruswami, J. Lee, and A. Wigderson. Euclidean sections with sublinear randomness and error-correction over the reals. In *Proceedings of the 12th International Workshop on Randomized Techniques in Computation*, pages 444–454, August 2008.
- [C16] V. Guruswami and P. Raghavendra. Constraint satisfaction over a non-boolean domain: Approximation algorithms and Unique Games hardness. In *Proceedings of the 11th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems*, pages 77–90, August 2008.
- [C17] V. Guruswami and A. Rudra. Soft decoding, dual BCH codes, and better list-decodable ϵ -biased codes. In *Proceedings of the 23rd IEEE Conference on Computational Complexity*, pages 163–174, June 2008.
- [C18] P. Gopalan and V. Guruswami. Hardness amplification within NP against deterministic algorithms. In *Proceedings of the 23rd IEEE Conference on Computational Complexity*, pages 19–30, June 2008.
- [C19] V. Guruswami and W. Machmouchi. Explicit interleavers for a Repeat Accumulate Accumulate (RAA) code construction. In *Proceedings of the International Symposium on Information Theory*, 2008.
- [C20] V. Guruswami and A. Rudra. Concatenated codes can achieve list decoding capacity. In *Proceedings of 19th ACM-SIAM Symposium on Discrete Algorithms*, pages 258–267, January 2008.
- [C21] V. Guruswami, J. Lee, and A. Razborov. Almost Euclidean sections of ℓ_1^n via expander codes. In *Proceedings of 19th ACM-SIAM Symposium on Discrete Algorithms*, pages 353–362, January 2008.
- [C22] V. Guruswami and A. Rudra. Better binary list-decodable codes via multilevel concatenation. In *Proceedings of the 11th International Workshop on Approximation, Randomization, and Combinatorial Optimization: Algorithms and Techniques*, pages 554–568, 2007.

- [C23] V. Guruswami, C. Umans, and S. P. Vadhan. Unbalanced expanders and randomness extractors from Parvaresh-Vardy codes. In *Proceedings of the 22nd IEEE Conference on Computational Complexity*, pages 96–108, 2007. Best paper award.
- [C24] V. Guruswami and P. Raghavendra. A 3-query PCP over integers. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 198–206, 2007.
- [C25] J. Chuzhoy, V. Guruswami, S. Khanna, and K. Talwar. Hardness of routing with congestion in directed graphs. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 165–178, 2007.
- [C26] V. Guruswami. On 2-query codeword testing. In *Proceedings of 17th International Symposium on Algorithms and Computation*, pages 267–276, December 2006.
- [C27] V. Guruswami and P. Raghavendra. Hardness of learning halfspaces with noise. In *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 543–552, October 2006.
- [C28] V. Guruswami and A. Patthak. Correlated Algebraic-Geometric codes: Improved list decoding over bounded alphabets. In *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 227–238, October 2006.
- [C29] V. Guruswami and A. Rudra. Explicit capacity-achieving list-decodable codes. In *Proceedings of the 38th Annual ACM Symposium on Theory of Computing (STOC)*, pages 1–10, May 2006.
- [C30] V. Guruswami and V. Kabanets. Hardness amplification via space-efficient direct products. In *Proceedings of the 7th Latin American Symposium on Theoretical Informatics – LATIN*, volume 3887 of *Lecture Notes in Computer Science*, pages 556–568. Springer, March 2006.
- [C31] P. Gopalan, V. Guruswami, and R. Lipton. Algorithms for modular counting of roots of multivariate polynomials. In *Proceedings of the 7th Latin American Symposium on Theoretical Informatics – LATIN*, volume 3887 of *Lecture Notes in Computer Science*, pages 544–555. Springer, March 2006.
- [C32] I. Giotis and V. Guruswami. Correlation clustering with a fixed number of clusters. In *Proceedings of the 17th ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1167–1176, January 2006.
- [C33] V. Guruswami and S. Vadhan. A lower bound on list size for list decoding. In *Proceedings of the 9th International Workshop on Randomization and Computation (RANDOM)*, pages 318–329, 2005.
- [C34] V. Guruswami and L. Trevisan. The complexity of making unique choices: Approximating 1-in- k SAT. In *Proc. of the 8th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems (APPROX)*, pages 99–110, 2005.

- [C35] V. Guruswami and A. Rudra. Tolerant locally testable codes. In *Proceedings of the 9th International Workshop on Randomization and Computation (RANDOM)*, pages 306–317, 2005.
- [C36] V. Guruswami and S. Khot. Hardness of Max 3SAT with no mixed clauses. In *Proceedings of the 20th IEEE Conference on Computational Complexity (CCC)*, pages 154–162, June 2005.
- [C37] V. Guruswami and A. Rudra. Limits to list decoding Reed-Solomon codes. In *Proceedings of the 37th ACM Symposium on Theory of Computing (STOC)*, pages 602–609, May 2005.
- [C38] V. Guruswami and A. Vardy. Maximum-Likelihood Decoding of Reed-Solomon codes is NP-hard. In *Proceedings of the 16th ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 470–478, January 2005.
- [C39] V. Guruswami, J. Hartline, A. Karlin, D. Kempe, C. Kenyon, and F. McSherry. On profit-maximizing envy-free pricing. In *Proceedings of the 16th ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1164–1173, January 2005.
- [C40] V. Guruswami and P. Indyk. Linear-time list decoding in error-free settings. In *Proceedings of the 31st International Colloquium on Automata, Languages and Programming (ICALP)*, pages 695–707, July 2004.
- [C41] V. Guruswami, D. Micciancio, and O. Regev. The complexity of the covering radius problem on lattices and codes. In *Proceedings of the 19th IEEE Conference on Computational Complexity (CCC)*, pages 161–173, June 2004.
- [C42] V. Guruswami. Better extractors for better codes? In *Proceedings of 36th Annual ACM Symposium on Theory of Computing (STOC)*, pages 436–444, June 2004.
- [C43] V. Guruswami and P. Indyk. Efficiently decodable codes meeting Gilbert-Varshamov bound for low rates. In *Proceedings of the 15th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 756–757, January 2004.
- [C44] M. Charikar, V. Guruswami, and A. Wirth. Clustering with qualitative information. In *Proceedings of the 44th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 524–533, October 2003.
- [C45] V. Guruswami. List decoding with side information. In *Proceedings of the 18th IEEE Conference on Computational Complexity (CCC)*, pages 300–309, July 2003.
- [C46] V. Guruswami and P. Indyk. Linear-time encodable and list decodable codes. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing (STOC)*, pages 126–135, June 2003.

- [C47] I. Dinur, V. Guruswami, S. Khot, and O. Regev. A new multilayered PCP and the hardness of hypergraph vertex cover. In *Proceedings of the 35th ACM Symposium on Theory of Computing (STOC)*, pages 595–601, June 2003.
- [C48] V. Guruswami and P. Indyk. Embeddings and non-approximability of geometric problems. In *Proceedings of the 14th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 537–538, 2003.
- [C49] V. Guruswami and I. Shparlinski. Unconditional proof of tightness of Johnson Bound. In *Proceedings of the 14th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 754–755, 2003.
- [C50] L. Engebretsen and V. Guruswami. Is constraint satisfaction over two variables always easy? In *6th International Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM)*, pages 224–238, 2002.
- [C51] V. Guruswami and M. Sudan. Decoding concatenated codes using soft information. In *Proceedings of the 17th Annual IEEE Conference on Computational Complexity (CCC)*, pages 148–157, 2002.
- [C52] V. Guruswami. Limits to list decodability of linear codes. In *Proceedings of the 34th Annual ACM Symposium on Theory of Computing (STOC)*, pages 802–811, 2002.
- [C53] V. Guruswami and P. Indyk. Near-optimal linear-time codes for unique decoding and new list-decodable codes over smaller alphabets. In *Proceedings of the 34th Annual ACM Symposium on Theory of Computing (STOC)*, pages 812–821, 2002.
- [C54] N. Alon, V. Guruswami, T. Kaufman, and M. Sudan. Guessing secrets efficiently via list decoding. In *Proceedings of the 13th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 254–262, 2002.
- [C55] V. Guruswami. List decoding from erasures: Bounds and code constructions. In *21st Foundations of Software Technology and Theoretical Computer Science*, pages 195–206, 2001.
- [C56] V. Guruswami. Constructions of codes from number fields. In *14th International Symposium on Applied Algebra, Algebraic Algorithms and Error Correcting Codes (AAECC)*, pages 129–140, 2001.
- [C57] V. Guruswami and P. Indyk. Expander-based constructions of efficiently decodable codes. In *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 658–667, 2001.
- [C58] V. Guruswami. Inapproximability results for set splitting and satisfiability problems with no mixed clauses. In *3rd International Workshop on Approximation Algorithms for Combinatorial Optimization Problems (APPROX)*, pages 155–166, 2000.

- [C59] V. Guruswami and M. Sudan. On representations of Algebraic-geometric codes for list decoding. In *Proceedings of the 8th Annual European Symposium on Algorithms*, pages 244–255, 2000.
- [C60] V. Guruswami, J. Håstad, and M. Sudan. Hardness of approximate hypergraph coloring. In *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 149–158, 2000.
- [C61] V. Guruswami, A. Sahai, and M. Sudan. ‘Soft-decision’ decoding of Chinese Remainder codes. In *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 159–168, 2000.
- [C62] M. Charikar, V. Guruswami, R. Kumar, S. Rajagopalan, and A. Sahai. Combinatorial feature selection problems. In *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 631–640, 2000.
- [C63] V. Guruswami and S. Khanna. On the hardness of 4-coloring a 3-colorable graph. In *Proceedings of the 15th IEEE Conference on Computational Complexity (CCC)*, pages 188–197, 2000.
- [C64] V. Guruswami and M. Sudan. List decoding algorithms for certain concatenated codes. In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (STOC)*, pages 181–190, 2000.
- [C65] M. Charikar, R. Fagin, V. Guruswami, J. M. Kleinberg, P. Raghavan, and A. Sahai. Query strategies for priced information. In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (STOC)*, pages 582–591, 2000.
- [C66] V. Guruswami, S. Khanna, R. Rajaraman, F. B. Shepherd, and M. Yannakakis. Near-optimal hardness results and approximation algorithms for Edge-disjoint Paths and related problems. In *Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC)*, pages 19–28, 1999.
- [C67] V. Guruswami and A. Sahai. Multiclass learning, Boosting, and Error-correcting codes. In *12th Annual Conference on Computational Learning Theory (COLT)*, pages 145–155, 1999.
- [C68] Y. Dodis, V. Guruswami, and S. Khanna. The 2-catalog segmentation problem. In *Proceedings of the 10th ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 897–898, 1999.
- [C69] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and Algebraic-geometric codes. In *Proceedings of the 39th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 28–39, 1998.

- [C70] V. Guruswami, D. Lewin, M. Sudan, and L. Trevisan. A tight characterization of NP with 3-query PCPs. In *Proceedings of the 39th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 8–17, 1998.
- [C71] V. Guruswami, C. P. Rangan, M. Chang, G. J. Chang, and C. K. Wong. The Vertex-disjoint Triangles problem. In *24th International Workshop on Graph-Theoretic Concepts in Computer Science (WG)*, pages 26–37, 1998.
- [C72] V. Guruswami, G. Mohan, and C. S. R. Murthy. Probabilistic routing in wavelength-routed multistage, hypercube, and debruijn networks. In *Proceedings of the 4th International Conference on High Performance Computing*, December 18-21, 1997.

Invited papers and surveys

- [I1] V. Guruswami. Bridging Shannon and Hamming: List error-correction with optimal rate. In *Proceedings of the International Congress of Mathematicians*, August 2010.
- [I2] V. Guruswami, J. Lee, and A. Wigderson. Expander codes over reals, Euclidean sections, and compressed sensing. In *Proceedings of the 47th Annual Allerton Conference on Communication, Control, and Computing*, October 2009.
- [I3] V. Guruswami. List decoding of binary codes – a brief survey of some recent results. In Y. M. Chee, C. Li, S. Ling, H. Wang, and C. Xing, editors, *IWCC*, volume 5557 of *Lecture Notes in Computer Science*, pages 97–106. Springer, 2009.
- [I4] V. Guruswami. List decoding and pseudorandom constructions. In *Proceedings of the 17th Symposium on Applied Algebra, Algebraic Algorithms, and Error Correcting Codes*, pages 1–6, December 2007.
- [I5] V. Guruswami and A. Rudra. Achieving list decoding capacity using folded Reed-Solomon codes. In *Proceedings of the 44th Annual Allerton Conference on Communication, Control, and Computing*, October 2006.
- [I6] V. Guruswami. Iterative Decoding of Low-Density Parity Check Codes. *Bulletin of the European Association for Theoretical Computer Science (EATCS)*, 90, October 2006.
- [I7] V. Guruswami. List Decoding in Pseudorandomness and Average-case Complexity. In *Proceedings of the IEEE Information Theory Workshop*, pages 32–36, March 2006.
- [I8] V. Guruswami. Error-correcting codes and expander graphs. *SIGACT News*, 35(3):25–41, September 2004.
- [I9] V. Guruswami and P. Indyk. Efficiently decodable codes meeting Gilbert-Varshamov bound for low rates. In *Proceedings of the 41st Annual Allerton Conference on Communication, Control, and Computing (Invited paper)*, pages 944–950, October 2003.

- [I10] V. Guruswami and M. Sudan. Reflections on 'Improved Decoding of Reed-Solomon and Algebraic-Geometric Codes'. *IEEE Information Theory Society Newsletter*, 52(1):6–12, March 2002.
- [I11] V. Guruswami and P. Indyk. Linear time codes to correct a maximum possible fraction of errors. In *Proceedings of the 39th Annual Allerton Conference on Communication, Control and Computing (Invited paper)*, 2001.
- [I12] V. Guruswami, J. Håstad, M. Sudan, and D. Zuckerman. Combinatorial bounds for list decoding. In *Proceedings of the 38th Annual Allerton Conference on Communication, Control and Computing (Invited paper)*, pages 602–612, October 2000.

CURRICULUM VITAE
Ioannis Kontoyiannis

Associate Professor, Department of Informatics
Athens University of Economics and Business

Department of Informatics
Athens University of Economics and Business
Patisision 76
Athens 10434, Greece

Phone: +30-210-8203-555
Fax: +30-210-8226-105
Email: yiannis@aueb.gr
Web: www.cs.aueb.gr/users/yiannisk/

EDUCATION

STANFORD UNIVERSITY, **Ph.D. Electrical Engineering.** June 1998.

Recurrence and Waiting Times in Stationary Processes, and their Applications in Data Compression.
Advisor: Prof. Thomas M. Cover. Associate Advisor: Prof. Amir Dembo.

STANFORD UNIVERSITY, **M.S. Statistics.** June 1997.

CAMBRIDGE UNIVERSITY, **M.S. Pure Mathematics.** June 1993.

Distinction in Part III of the Cambridge Mathematics Tripos.

IMPERIAL COLLEGE, UNIVERSITY OF LONDON, **B.S. Mathematics.** June 1992.

First Class Honors.

PROFESSIONAL APPOINTMENTS

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS (Greece)

March 2004 – present

Associate Professor, Department of Informatics.

BROWN UNIVERSITY (USA)

July 2004 – July 2005

Associate Professor (with tenure), Division of Applied Mathematics and (jointly) Department of Computer Science.

BROWN UNIVERSITY (USA)

Oct. 2002 – July 2004

Manning Assistant Professor, Division of Applied Mathematics and (jointly) Department of Computer Science.

BROWN UNIVERSITY (USA)

Aug. 2001 – July 2004

Assistant Professor, Division of Applied Mathematics and (jointly) Department of Computer Science.

PURDUE UNIVERSITY (USA)

Aug. 1998 – Aug. 2001

Assistant Professor, Department of Statistics, and (by courtesy) Department of Mathematics, and the School of Electrical and Computer Engineering.

IBM T.J. WATSON RESEARCH CENTER (USA)

June 1995 – Dec. 1995

Research Co-op. Worked on the IBM-NASA Satellite Image Explorer Project. Research in image processing, classification and compression algorithms.

RESEARCH INTERESTS

Probability and stochastic processes, information theory, data compression, statistics, communications and signal processing, mathematical biology

VISITING POSITIONS

- COLUMBIA UNIVERSITY *Jan. 2008 – Dec. 2008*
Visiting Associate Professor, Department of Statistics.
- BROWN UNIVERSITY *July 2005 – July 2007*
Visiting Associate Professor (Research), Division of Applied Mathematics.
- BROWN UNIVERSITY *September 2002 – July 2007*
Visiting Research Associate, Computation and Mathematics of Mind (under NSF's IGERT Program),
 Department of Neuroscience.
- ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS *Sept. 2004 – Feb. 2005*
Visiting Associate Professor, Department of Informatics.
- BROWN UNIVERSITY *Aug. 2000 – July 2001*
Visiting Assistant Professor, Division of Applied Mathematics.
- CAMBRIDGE UNIVERSITY *July 1999, June '98, June '97, Aug. '96, June '95, Sept. '93*
Visiting Scholar, Statistical Laboratory (Dept of Pure Mathematics and Mathematical Statistics).

PUBLICATIONS

JOURNAL PAPERS

Submitted

1. A. Anagnostopoulos, C. Dombry, N. Guillotin-Plantard, I. Kontoyiannis and E. Upfal. “Probabilistic analysis of the k -server problem on the circle.” Submitted.
2. I. Kontoyiannis and S.P. Meyn. “Geometric ergodicity and the spectral gap of non-reversible Markov chains.” Submitted.
3. C. Gioran and I. Kontoyiannis. “Lossy compression in near-linear time via efficient random codebooks and databases.” Submitted.
4. P. Dellaportas and I. Kontoyiannis. “Control variates for reversible MCMC samplers.” Submitted.
5. I. Kontoyiannis and S.P. Meyn. “Approximating a diffusion by a hidden Markov model.” Submitted.
6. O. Johnson, I. Kontoyiannis and M. Madiman. “Log-concavity, ultra-log-concavity and a maximum entropy property of discrete compound Poisson measures.” Submitted.

Published or in press

7. P. Harremoës, O. Johnson and I. Kontoyiannis “Thinning, entropy and the law of thin numbers.” *IEEE Transactions on Information Theory*, **56**, no. 9, pp. 4228–4244, September 2010.
8. A.D. Barbour, O. Johnson, I. Kontoyiannis and M. Madiman. “Compound Poisson approximation via information functionals.” *Electronic Journal of Probability*, **15**, paper 42, pp. 1344–1369, August 2010.
9. I. Kontoyiannis. “Book review: “*Information and complexity in statistical modeling*,” by J. Rissanen, Springer, NY, 2007.” *Amer. Math. Monthly*, **115**, no. 10, pp. 956–960, December 2008.
10. I. Kontoyiannis and S.P. Meyn. “Computable exponential bounds for screened estimation and simulation.” *Annals of Applied Probability*, **18**, no. 4, pp. 1491–1518, August 2008.
11. M. Harrison and I. Kontoyiannis. “Estimation of the rate-distortion function.” *IEEE Transactions on Information Theory*, **54**, no. 8, pp. 3757–3763, August 2008.
12. Y. Gao, I. Kontoyiannis and E. Bienenstock. “Estimating the entropy of binary time series: Methodology, some theory and a simulation study.” *Entropy*, **10**, issue 2, pp. 71–99, June 2008.
13. I. Kontoyiannis. “Counting the primes using entropy.” *IEEE Information Theory Newsletter*, **58**, no. 2, pp. 6–9, June 2008.
14. H.M. Aktulga, I. Kontoyiannis, L.A. Lyznik, L. Szpankowski, A.Y. Grama and W. Szpankowski. “Identifying statistical dependence in genomic sequences via mutual information estimates.” In *EURASIP Journal on Bioinformatics and Systems Biology*, **vol. 2007**, article ID 14741, November 2007.
15. I. Kontoyiannis and M. Madiman. “Measure concentration for compound Poisson distributions.” *Electronic Communications in Probability*, **11**, paper 5, pp. 45–57, May 2006.
16. I. Kontoyiannis and R. Zamir. “Mismatched codebooks and the role of entropy-coding in lossy data compression.” *IEEE Transactions on Information Theory*, **52**, pp. 1922–1938, May 2006.
17. A. Anagnostopoulos, I. Kontoyiannis, and E. Upfal. “Steady state analysis of balanced-allocation routing,” *Random Structures & Algorithms*, **26**, pp. 446–467, July 2005.

18. I. Kontoyiannis and S.P. Meyn. “Large deviations asymptotics and the spectral theory of multiplicatively regular Markov processes,” *Electronic Journal of Probability*, **10**, paper 3, pp. 61–123, February 2005.
19. I. Kontoyiannis, P. Harremoës and O. Johnson. “Entropy and the law of small numbers,” *IEEE Transactions on Information Theory*, **51**, pp. 366–472, February 2005.
20. I. Kontoyiannis. “Pattern matching and lossy data compression on random fields,” *IEEE Transactions on Information Theory*, **49**, pp. 1047–1051, April 2003.
21. N. Merhav and I. Kontoyiannis. “Source coding exponents for zero-delay coding with finite memory,” *IEEE Transactions on Information Theory*, **49**, pp. 609–625, March 2003.
22. I. Kontoyiannis and S.P. Meyn. “Spectral theory and limit theorems for geometrically ergodic Markov processes,” *Annals of Applied Probability*, **13**, pp. 304–362, February 2003.
23. I. Kontoyiannis and J. Zhang. “Arbitrary source models and Bayesian codebooks in rate-distortion theory,” *IEEE Transactions on Information Theory*, **48**, pp. 2276–2290, August 2002.
24. A. Dembo and I. Kontoyiannis. “Source coding, large deviations, and approximate pattern matching.” Invited paper in the special issue of the *IEEE Transactions on Information Theory* on Shannon Theory, dedicated to A.D. Wyner, **48**, pp. 1590–1615, June 2002.
25. A. Antos and I. Kontoyiannis. “Convergence properties of functional estimates for discrete distributions,” *Random Structures & Algorithms*, **9**, pp. 163–193, October 2001, special issue in honor of D.E. Knuth’s 64th birthday.
26. J. Zhang, E.K.P. Chong and I. Kontoyiannis. “Unified spatial diversity combining and power allocation schemes for CDMA systems,” *IEEE Journal on Selected Areas in Communications*, **19**, pp. 1276–1288, July 2001.
27. I. Kontoyiannis. “Sphere-covering, measure concentration, and source coding,” *IEEE Transactions on Information Theory*, **46**, pp. 1544–1552, May 2001.
28. A. Dembo and I. Kontoyiannis. “Critical behavior in lossy source coding,” *IEEE Transactions on Information Theory*, **46**, pp. 1230–1236, March 2001.
29. I. Kontoyiannis. “Pointwise redundancy in lossy data compression and universal lossy data compression,” *IEEE Transactions on Information Theory*, **46**, pp. 136–152, January 2000.
30. I. Kontoyiannis. “An implementable lossy version of the Lempel-Ziv algorithm – Part I: Optimality for memoryless sources,” *IEEE Transactions on Information Theory*, **45**, pp. 2293–2305, November 1999.
31. A. Dembo and I. Kontoyiannis. “The asymptotics of waiting times between stationary processes, allowing distortion,” *Annals of Applied Probability*, **9**, pp. 413–429, May 1999.
32. I. Kontoyiannis. “Asymptotic recurrence and waiting times for stationary processes,” *Journal of Theoretical Probability*, **11**, pp. 795–811, July 1998.
33. I. Kontoyiannis, P.H. Algoet, Yu.M. Suhov and A.J. Wyner. “Nonparametric entropy estimation for stationary processes and random fields, with applications to English text,” *IEEE Transactions on Information Theory*, **44**, pp. 1319–1327, May 1998.
34. V. Castelli, L. Bergman, I. Kontoyiannis, C.-S. Li, J. Robinson and J. Turek. “Progressive search and retrieval in large image archives,” *IBM Journal of Research and Development*, **42**, pp. 253–268, March 1998.

35. I. Kontoyiannis. “Second-order noiseless source coding theorems,” *IEEE Transactions on Information Theory*, **43**, pp. 1339–1341, July 1997.

BOOK CHAPTERS

36. I. Kontoyiannis. “Some information-theoretic computations related to the distribution of prime numbers,” In *Festschrift in Honor of Jorma Rissanen*, (P. Grunwald, P. Myllymaki, I. Tabus, M. Weinberger, B. Yu, eds.), pp. 135–143, Tampere University Press, May 2008.
37. I. Kontoyiannis and Yu.M. Suhov. “Prefixes and the entropy rate for long-range sources,” Chapter 6 in *Probability Statistics and Optimization: A Tribute to Peter Whittle*, (F.P. Kelly, editor), pp. 89–98, Wiley, Chichester, 1994.

PATENTS

38. V. Castelli, I. Kontoyiannis, J. Robinson and J.J. Turek. U.S. Patent No. 6,021,224. “Multiresolution lossless/lossy compression and storage of data for efficient processing thereof.” Oct 2000.
39. V. Castelli, I. Kontoyiannis, J. Robinson and J.J. Turek. U.S. Patent No. 6,141,445. “Multiresolution lossless/lossy compression and storage of data for efficient processing thereof.” Feb 2000.

UNPUBLISHED MANUSCRIPTS

40. P. Dellaportas and I. Kontoyiannis “Notes on using control variates for estimation with reversible MCMC samplers,” *arXiv online manuscript*, July 2009.
41. V. Castelli and I. Kontoyiannis. “An efficient recursive partitioning algorithm for classification, using wavelets,” *APPTS Technical Report #02-7*, Brown University, September 2002.
42. I. Kontoyiannis. “The complexity and entropy of literary styles.” *NSF Technical Report no. 97*, Department of Statistics, Stanford University, June 1996.
43. I. Kontoyiannis, J. Turek, V. Castelli and J. Robinson. “Multiresolution lossless image compression.” Unpublished manuscript, December 1995.

CONFERENCES (papers/talks)

- C1. “Geometric ergodicity and the spectral gap of non-reversible Markov chains,” with Sean P. Meyn. **Invited talk**, *Fifth International Workshop on Applied Probability*, Madrid, Spain, July 2010.
- C2. “Stochastic analysis of the k -server problem on the circle,” with A. Anagnostopoulos, C. Dombry, N. Guillin-Plantard and E. Upfal. *21st International Meeting on Probabilistic, Combinatorial and Asymptotic Methods for the Analysis of Algorithms (AofA 2010)*, June-July 2010.
- C3. “The entropies of the sum and the difference of two IID random variables are not too different,” with M. Madiman. *2010 IEEE International Symposium on Information Theory*, Austin, TX, June 2010.
- C4. “Simulating the mean of a skip-free Markov chain,” with K.R. Duffy and S.P. Meyn. *Simulation of Networks Workshop*, Cambridge University, UK, June 2010.
- C5. “Superpositions codes for Gaussian vector quantization,” with K. Rahnama Rad and S. Gitzenis. **Invited paper**, *2010 IEEE Information Theory Workshop*, Cairo, Egypt, January 2010.
- C6. “Which spectrum?” with S.P. Meyn. **Invited talk**, *Athens Workshop on MCMC Convergence and Estimation*, Athens, Greece, September 2009.
- C7. “Three non-asymptotic results in source coding and probability.” **Plenary talk**, *2009 Workshop on Information Theoretic Methods in Science and Engineering*, Tampere, Finland, August 2009.

- C8. “Waiting and matching: Patterns and entropy.” **Invited series of talks**, *Greek Stochastics α'* , Lefkada, Greece, August 2009.
- C9. “Control variates for MCMC.” *Greek Stochastics α'* , with P. Dellaportas and Z. Tsourti. Lefkada, Greece, August 2009.
- C10. “A criterion for the compound Poisson distribution to be maximum entropy,” with O. Johnson and M. Madiman. *2009 IEEE International Symposium on Information Theory*, Seoul, Korea, July 2009.
- C11. “Efficient random codebooks and databases for lossy data compression,” with C. Gioran. **Invited paper**, *2009 IEEE Information Theory Workshop*, Volos, Greece, June 2009.
- C12. “Information-theoretic ideas in Poisson approximation and estimation.” **Invited talk**, *Interface between Information Theory and Estimation Theory Workshop*, Princeton University, April 2009.
- C13. “Control variates as screening functions,” with S. Kyriazopoulou-Panagiotopoulou and S.P. Meyn. *Third International Conference on Performance Evaluation Methodologies and Tools*, Athens, Greece, October 2008.
- C14. “An information-theoretic development of compound Poisson approximation,” with A.D. Barbour, O. Johnson and M. Madiman. **Invited talk**, *Second EPFL-UMLV International Workshop on Entropy*, Lausanne, Switzerland, September 2008.
- C15. “Entropy and the ‘compound’ law of small numbers.” with O. Johnson and M. Madiman. **Invited talk**, *2008 Workshop on Information Theoretic Methods in Science and Engineering*, Tampere, Finland, August 2008.
- C16. “Information-theoretic bounds for compound Poisson approximation,” with A.D. Barbour, O. Johnson and M. Madiman. *7th World Congress in Probability and Statistics*, Singapore, July 2008.
- C17. “Thinning and information projections,” with P. Harremöes and O. Johnson. *2008 IEEE International Symposium on Information Theory*, Toronto, Canada, July 2008.
- C18. “Counting the primes using entropy.” **Invited paper**, *2008 IEEE Information Theory Workshop*, Porto, Portugal, May 2008.
- C19. “On the spectral theory of Markov chains.” *12th Panhellenic Conference in Mathematical Analysis*, Athens, Greece, May 2008.
- C20. “Statistical dependence in biological sequences,” with H.M. Aktulga, L.A. Lyznik, L. Szpankowski, A.Y. Grama and W. Szpankowski. *2007 IEEE International Symposium on Information Theory*, Nice, France, June 2007.
- C21. “Thinning and the law of small numbers,” with P. Harremoës and O. Johnson. *2007 IEEE International Symposium on Information Theory*, Nice, France, June 2007.
- C22. “Fisher information, compound Poisson approximation, and the Poisson channel,” with M. Madiman and O. Johnson. *2007 IEEE International Symposium on Information Theory*, Nice, France, June 2007.
- C23. “Exponential bounds and stopping rules for MCMC and general Markov chains,” with L.A. Lastras-Montaño and S.P. Meyn. **Invited paper**, *First International Conference on Performance Evaluation Methodologies and Tools*, Pisa, Italy, October 2006.
- C24. “Information-theoretic ideas in Poisson approximation and concentration.” **Invited series of talks**, *LMS/EPSRC Meeting on Stochastic Stability, Large Deviations and Coupling Methods*, Edinburgh, UK, September 2006.
- C25. “On estimating the rate-distortion function,” with M. Harrison. *2006 IEEE International Symposium on Information Theory*, Seattle, WA, July 2006.
- C26. “From the entropy to the statistical structure of spike trains,” with Y. Gao and E. Bienenstock. *2006 IEEE International Symposium on Information Theory*, Seattle, WA, July 2006.
- C27. “Entropy estimation: Simulation, theory and a case study.” **Invited paper**, *2006 IEEE Information Theory Workshop*, Punta del Este, Uruguay, March 2006.

- C28. “From Poisson approximation to compound Poisson concentration via entropy.” **Invited talk**, *First EPFL-UMLV International Workshop on Entropy*, Lausanne, Switzerland, February 2006.
- C29. “Combining information from different sources: Some surprising phenomena,” with B. Lucena. **Invited paper**, *10th Panhellenic Conference on Informatics*, Volos, Greece, November 2005.
- C30. “Filtering: The case for *noisier* data,” with B. Lucena. *2005 IEEE Information Theory Workshop*, Rotorua, New Zealand, September 2005.
- C31. “Mutual information, synergy and some curious phenomena for simple channels,” with B. Lucena. *2005 IEEE International Symposium on Information Theory*, Adelaide, Australia, September 2005.
- C32. “Relative entropy and exponential deviation bounds for general Markov chains,” with L. Lastras-Montaño and S.P. Meyn. *2005 IEEE International Symposium on Information Theory*, Adelaide, Australia, September 2005.
- C33. “Concentration and relative entropy for compound Poisson distributions,” with M. Madiman. *2005 IEEE International Symposium on Information Theory*, Adelaide, Australia, September 2005.
- C34. “Sobolev inequalities, Poisson approximation and concentration,” **Invited paper**, *7th Hellenic European Conference on Computer Mathematics & its Applications*, Athens, Greece, September 2005.
- C35. “Entropy, compound Poisson approximation, log-Sobolev inequalities and measure concentration,” with M. Madiman. *2004 IEEE Information Theory Workshop*, San Antonio, TX, October 2004.
- C36. “Minimum Description Length vs. Maximum Likelihood in lossy data compression,” with M. Harrison and M. Madiman. *IEEE International Symposium on Information Theory*, Chicago, IL, July 2004.
- C37. “Estimating the entropy rate of spike trains,” with Y. Gao and E. Bienenstock. **Invited paper**, *38th Annual Conference on Information Sciences and Systems*, Princeton, NJ, March 2004.
- C38. “Poisson approximation via entropy,” with P. Harremoës and O. Johnson. *Second International Workshop on Applied Probability*, Piraeus, Greece, March 2004.
- C39. “Lempel-Ziv and CTW entropy estimators for spike trains,” with Y. Gao and E. Bienenstock. **Invited paper**, *Estimation of entropy Workshop, 2003 Neural Information Processing Systems Conference*, Vancouver, BC, Canada, December 2003.
- C40. “The advantage of balanced-allocation routing for ATM networks,” with A. Anagnostopoulos and E. Ufpa. *2003 IEEE International Symposium on Information Theory*, Yokohama, Japan, July 2003.
- C41. “Mismatched codebooks and the role of entropy-coding in lossy data compression,” with R. Zamir. *2003 IEEE International Symposium on Information Theory*, Yokohama, Japan, July 2003.
- C42. “Entropy and the law of small numbers,” with P. Harremoës. *2003 IEEE International Symposium on Information Theory*, Yokohama, Japan, July 2003.
- C43. “Maximum likelihood estimation for lossy data compression,” with M. Harrison. **Invited paper**, *40th Annual Allerton Conference on Communication, Control, and Computing*, Allerton, IL, October 2002.
- C44. “Source coding exponents for zero-delay coding with finite memory,” with N. Merhav. *2002 IEEE International Symposium on Information Theory*, Lausanne, Switzerland, July 2002.
- C45. “Arbitrary source models and Bayesian codebooks in rate-distortion theory,” with J. Zhang. *2002 IEEE International Symposium on Information Theory*, Lausanne, Switzerland, July 2002.

- C46. “Unified error exponents: Hypothesis testing, data compression, and measure concentration,” with A.D. Sezer. **Invited paper**, *Barcelona Conference on Stochastic Inequalities and Their Applications*, Spain, June 2002; published in *Progress in Probability*, vol. 56, pp. 23–32, Birkhauser Basel/Switzerland, 2003.
- C47. “MDL ideas in lossy data compression.” **Invited talk**, *MSRI Information Theory Workshop*, Berkeley, CA, March 2002.
- C48. “The ODE method and spectral theory of Markov operators,” with J. Huang and S.P. Meyn. **Invited paper**, *Proceedings of the Stochastic Theory and Control Workshop*, Springer, New York, pp. 205–221, B. Pasik-Duncan (Editor), 2002.
- C49. “Precise limit theorems and multiplicative ergodicity for Markov processes,” with S.P. Meyn. *11th INFORMS Applied Probability Society Conference*, New York, NY, July 2001.
- C50. “Limit theorems and some spectral theory for geometrically ergodic Markov chains.” **Plenary talk**, *Conference on Stochastic Processes and their Applications*, Cambridge, UK, July 2001.
- C51. “Sphere-covering and measure concentration as source coding theorems.” *2001 IEEE International Symposium on Information Theory*, Washington, D.C., June 2001.
- C52. “Estimating the entropy of discrete distributions,” with A. Antos. *2001 IEEE International Symposium on Information Theory*, Washington, D.C., June 2001.
- C53. “Unified spatial diversity combining and power allocation schemes for CDMA systems,” with J. Zhang and E.K.P. Chong. *GLOBECOM 2000*, San Francisco, CA, December 2000.
- C54. “Critical behavior in source coding,” with A. Dembo. *2000 International Symposium on Information Theory and Its Applications*, Honolulu, Hawaii, November 2000.
- C55. “On rate-distortion theory as a convex selection problem.” **Invited paper**, *38th Annual Allerton Conference on Communication, Control & Computing*, October 2000.
- C56. “Probabilistic phenomena in data compression.” **Invited talk** at the *Sixth International Seminar on the Analysis of Algorithms*, Krynica Morska, Poland, July 2000.
- C57. “Model selection via rate-distortion theory.” **Invited paper**, *34th Annual Conference on Information Sciences and Systems*, Princeton, NJ, March 2000.
- C58. “Probabilistic results for sphere packing in high dimensions.” *1999 Joint Statistical Meetings of IMS-ASA-ENAR/WNAR*, Baltimore, MD, August 1999.
- C59. “How well does the Shannon codebook compress?” *1999 Canadian Information Theory Workshop*, Kingston, Ontario, June 1999.
- C60. “Asymptotically optimal lossy Lempel-Ziv coding.” *1998 IEEE International Symposium on Information Theory*, MIT, Cambridge, MA, August 1998.
- C61. “Generalized waiting times and efficient lossy coding for memoryless sources.” *1998 IEEE Information Theory Workshop*, San Diego, CA, February 1998.
- C62. “Second-order analysis of lossless and lossy versions of Lempel-Ziv codes.” **Invited paper**, *31st Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, November 1997.
- C63. “The asymptotics of waiting times between stationary processes.” *1997 Joint Statistical Meeting of IMS-ASA-ENAR/WNAR*, Anaheim, CA, August 1997.
- C64. “On the distribution of recurrence times and the exact asymptotics of Lempel-Ziv coding.” *1997 IEEE International Symposium on Information Theory*, Ulm, Germany, June–July 1997.
- C65. “Two refinements to Shannon’s source coding theorem.” *1997 IEEE International Symposium on Information Theory*, Ulm, Germany, June–July 1997.
- C66. “Progressive classification in the compressed domain for large EOS satellite databases,” with V. Castelli, C.S. Li and J.J. Turek. *1996 IEEE International Conference on Acoustics, Speech and Signal Processing*, Atlanta, GA, May 1996.

- C67. “Stationary entropy estimation via string matching,” with Yu.M. Suhov. *The Data Compression Conference DCC 96*, Snowbird, UT, April 1996.
- C68. “Prefixes and the entropy rate for long-range sources,” with Yu.M. Suhov. *1994 IEEE International Symposium on Information Theory*, Trondheim, Norway, June 1994.

SELECTED INVITED TALKS

- “*Geometric Ergodicity and the Spectral Gap of Non-reversible Markov Chains.*”
Fifth International Workshop on Applied Probability, Madrid, Spain, July 2010.
- “*Sunset Entropy Theory.*”
Information Theory Summer School, Chania, Greece, July 2010.
- “*Non-Asymptotics: Probability, Entropy and Additive Combinatorics.*”
Invited Lectures, Statistics Dept., Columbia Univ., June 2010.
- “*Superposition Codes for Gaussian Vector Quantization.*”
2010 IEEE Information Theory Workshop, Cairo, Egypt, January 2010.
- “*Which Spectrum?*”
Athens Workshop on MCMC Convergence and Estimation, Athens, Greece, September 2009.
- “*Three Non-Asymptotic Results in Source Coding and Probability.*”
Plenary talk, Workshop on Info-Theoretic Methods in Sci. & Eng’ng, Finland, Aug 2009.
- “*Efficient Random Codebooks for Lossy Compression of Binary Data.*”
2009 IEEE Information Theory Workshop, Volos, Greece, June 2009.
- “*Waiting and Matching: Patterns and Entropy.*”
 Short course at **Greek Stochastics α'** , Lefkada, Greece, August 2009.
- “*Variance Reduction via Control Variates in MCMC Estimation.*”
 Statistics Seminar, **Yale University**, April 2009.
- “*Information-Theoretic Ideas in Poisson Approximation and Estimation.*”
Interface between Information Theory & Estimation Workshop, Princeton U., April 2009.
- “*Control Variates for Reversible MCMC Samplers.*”
 Statistics Seminar, **Columbia University**, February 2009.
- “*Recurrence, Waiting Times, and Pattern-Matching in Information Theory.*”
 Short course at **EURANDOM Workshop**, Eindhoven, The Netherlands, November 2008.
- “*An Information-Theoretic Development of Compound Poisson Approximation.*”
Second EPFL-UMLV International Workshop on Entropy, Lausanne, Switzerland, Sept. 2008.
- “*Entropy and the ‘Compound’ Law of Small Numbers.*”
Workshop on Information-Theoretic Methods in Science & Engineering, Finland, Aug 2008.
- “*Counting the Primes Using Entropy.*”
2008 IEEE Information Theory Workshop, Porto, Portugal, May 2008.
- “*Computable Exponential Bounds for Markov Chains and MCMC Simulation.*”
 Probability Seminar, **Columbia University**, December 2007.
- “*Exponential Bounds and Stopping Rules for MCMC and General Markov Chains.*”
First ValueTools Conference, Pisa, Italy, October 2006.

- “*Information-Theoretic Ideas in Poisson Approximation and Concentration*,”
LMS/EPSRC Meeting on Stochastic Stability, Edinburgh, UK, September 2006.
- “*Entropy Estimation: Simulation, Theory and a Case Study*.”
2006 IEEE Information Theory Workshop, Punta del Este, Uruguay, March 2006.
- “*From Poisson Approximation to Compound Poisson Concentration via Entropy*.”
First EPFL-UMLV International Workshop on Entropy, Lausanne, Switzerland, February 2006.
- “*Combining Information from Different Sources: Some Surprising Phenomena*.”
10th Panhellenic Conference on Informatics, Volos, Greece, Nov 2005.
- “*Sobolev Inequalities, Poisson Approximation and Concentration*.”
HERCMA Conference 2005, Athens, Greece, September 2005.
- “*A Statistical Foundation for Lossy Data Compression*.”
Telecommunications Forum, **Telecom Research Centre & Vienna Univ of Technology**, Dec 2004.
- “*Poisson Approximation and Poisson Concentration Via Entropy*.”
Swiss Probability Seminar, Bern, Switzerland, November 2004.
- “*Poisson Approximation and Entropy*.”
Mathematics Dept Seminar, **University of Patras, Greece**, September 2004.
- “*Poisson Approximation Via Entropy*.”
Mathematics Seminar, **Univ of Illinois, Urbana-Champaign**, June 2004.
- “*Entropy, Compound Poisson Approximation and Log-Sobolev Inequalities*.”
Statistics Seminar, **University of Chicago**, June 2004.
- “*Investment and Data Compression: Universal Portfolios*.”
Summer School on Financial Mathematics, **Athens University**, Nafplio, Greece, July 2004.
- “*Large Deviations, Multiplicative Ergodicity and Spectral Theory for Markov Chains*.”
Joint Probability and Applied Math Seminar, **Stanford University**, October 2003.
- “*Limit Theorems and Some Spectral Theory for Geometrically Ergodic Markov Processes*.”
Statistics Seminar, **University of Chicago**, February 2003.
- “*Geometrically Ergodic Markov Chains: Limit Theorems and Analytical Structure*.”
Mathematics Seminar, **National Technical University of Athens**, Greece, January 2003.
- “*Probabilistic Pattern Matching and Its Applications*.”
Management Sciences Lab Research Seminar, **Athens Univ of Economics & Business**, July 2002.
- “*Unified Error Exponents: Hypothesis Testing, Data Compression & Measure Concentration*.”
Barcelona Conference on Stochastic Inequalities and Their Applications, Spain, June 2002.
- “*Statistical Lossy Data Compression*.”
Symbol Technologies Lecturer, Brooklyn Polytechnic, ECE Department, March 2002.
- “*Limit Theorems and Some Spectral Theory for Geometrically Ergodic Markov Processes*.”
Probability Seminar, **Columbia University**, March 2002.
- “*MDL Ideas in Lossy Data Compression*.”
MSRI Information Theory Workshop, Berkeley, CA, March, 2002.
- “*On the Convergence of Geometrically Ergodic Markov Chains*.”
Joint Statistics Colloquium/Probability Seminar **Stanford University**, February 2002.

- “*Limit Theorems and Some Spectral Theory for Geometrically Ergodic Markov Processes.*”
Probability seminar, **Purdue University**, October 2001.
- “*Probabilistic Aspects of Pattern Matching in Genetics and in Data Compression.*”
Bioinformatics/Statistical Genomics Seminar, **Purdue University**, October 2001
- “*On the Role of Memory in Data Compression.*”
Communications Seminar, **Univ of Illinois, Urbana-Champaign**, October 2001.
- “*Limit Theorems and Some Spectral Theory for Geometrically Ergodic Markov Processes.*”
Plenary talk, Conference on Stochastic Processes & Applications, Cambridge, UK, July 2001.
- “*On Rate-Distortion Theory as a Convex Selection Problem.*”
38th Annual Conference on Communication, Control & Computing, Allerton, October 2000.
- “*Probabilistic Phenomena in Data Compression.*”
Sixth International Seminar on the Analysis of Algorithms, Poland, July 2000.
- “*Model Selection via Rate-Distortion Theory.*”
34th Annual Conference on Information Sciences and Systems, Princeton, March 2000.
- “*How Well Can We Compress?*”
Network Modelling and Control Seminar, **Univ of Illinois, Urbana-Champaign**, February 2000.
- “*Measure Concentration, Combinatorial Optimization and Data Compression.*”
Statistics Seminar, **Cambridge University**, July 1999.
- “*Combinatorial Optimization, Measure Concentration and Data Compression.*”
Joint IEOR – Management Science Colloquium, **Columbia University**, April 1999.
- “*How Fast Can We compress?*”
Networking and Communications Seminar, **University of California, Berkeley**, February 1999.
- “*Sphere-Packing Questions with Probabilistic Answers.*”
Probability and Stochastic Processes Seminar, **Stanford University**, February 1999.
- “*Waiting Times, String Matching and Data Compression.*”
Statistics Seminar, **Cambridge University**, July 1998.
- “*An Implementable Version of Lossy Lempel-Ziv Coding that is Compression-Optimal.*”
Research Seminar, **Hewlett-Packard Research Laboratories**, Palo Alto, June 1998.
- “*Pattern Recurrence in Stationary Processes.*”
Statistics Colloquium, **University of California, Berkeley**, March 1998.
- “*Efficient Universal Data Compression.*”
Networking and Communications Seminar, **University of California, Berkeley**, February 1998.
- “*Second-Order Analysis of Lossless and Lossy Versions of Lempel-Ziv Codes.*”
31st Asilomar Conference on Signals, Systems and Computers, November 1997.
- “*Recurrence and the Entropy of Stationary Processes.*”
Statistics Seminar, **Cambridge University**, August 1996.

AWARDS, GRANTS, DISTINCTIONS

PLENARY SPEAKER

International Workshop on Information-Theoretic Methods in Science and Engineering, Tampere, Finland, August 2009.

MARIE CURIE FELLOW

International Outgoing Fellowship, Marie Curie Program (EU), entitled *Control Variates for Markov Chain Monte Carlo Variance Reduction*, 2009 – 2011. [~**Euro 200,000**].

AUEB “BASIC RESEARCH” GRANT

AUEB Basic Research (PEVE) grant entitled *Simulation, computational learning and hypothesis testing: Theory and algorithms for efficient statistical computation*, 2009 – 2010. [~**EURO 10,000**].

EU RESEARCH GRANT

Investigator on European Union research grant entitled *Novel issues and techniques for the analysis of hyperlink structure on the WWW graph*, 2006 – 2008. [~**\$20,000**].

HONORARY MASTER OF ARTS DEGREE, AD EUNDEM

Awarder by Brown University, May 2005.

SLOAN RESEARCH FELLOWSHIP

Awarder by the Sloan Foundation, March 2004.

MANNING ASSISTANT PROFESSORSHIP

Endowed assistant professorship, awarder by Brown University, October 2002.

PLENARY SPEAKER

Conference on Stochastic Processes and their Applications, Cambridge, UK, July 2001.

NSF RESEARCH GRANT

PI on NSF research grant entitled *Efficient lossy data compression via statistical model selection*, July 2000 – June 2004, under the Communications Research Program. [~**\$100,000**].

USDA RESEARCH GRANT

Co-PI with R.W. Doerge and L.M. McIntyre (Genomics, Purdue Univ.) on four-year USDA grant entitled *Development of statistical methodology for agricultural genomics*, beginning October 1, 2000, under the Initiative for Future Agriculture and Food Systems (IFAFS) Program. [~**\$1,000,000**].

TEACHING FOR TOMORROW AWARD

Received (Spring 2000) the annual Purdue Teaching for Tomorrow Award, which “recognizes young faculty members for their commitment to and accomplishments in teaching and student learning.”

SUMMER FACULTY GRANT

Awarded by the Purdue Research Foundation. Summer support for 1999.

PURDUE GLOBAL INITIATIVE FACULTY GRANT

Miscellaneous research support for the “Purdue Mini-Seminar on Information Theory,” held in April–May 1999. Awarded by the Purdue Research Foundation. [**\$10,000**].

RESEARCH GRANT

Student support from the Purdue Research Foundation, for a research student for two years. [~**\$25,000**].

PROFESSIONAL ACTIVITIES

ASSOCIATE EDITOR *Acta Applicandae Mathematicae*, published by Springer, 2010–2013.

ASSOCIATE EDITOR *IEEE Transactions on Information Theory* in the area of Shannon Theory, 2007–2010.

EDITORIAL COMMITTEE *Quarterly of Applied Mathematics*, published by the American Mathematical Society, 2004–present.

EDITORIAL BOARD *Entropy Journal* (Electronic) ISSN 1099-4300, 1999–2008.

URL: www.mdpi.org/entropy

IEEE INFORMATION THEORY SOCIETY AWARDS COMMITTEE

Member of the committee, which is responsible, among others, for the *Information Theory Society Best Paper Award*, the *Joint Information Theory-Communications Society Best Paper Award* and the *ISIT Student Paper Award*

CONFERENCE TECHNICAL PROGRAM CO-CHAIR

IEEE Workshop on Information Theoretic Methods in Science and Engineering (2008, 2009, 2010)

IEEE Information Theory Workshop (2009)

CONFERENCE GENERAL CO-CHAIR

Athens Workshop on MCMC Convergence and Estimation (2009)

Greek Stochastics (α' 2009, β' 2010)

CONFERENCE PROGRAM COMMITTEE

IEEE Communication Theory Symposium of the *IEEE Int. Conference on Communications* (2010)

IEEE International Symposium on Information Theory (2008, 2009, 2010, 2011)

IEEE Int. Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (2009)

IEEE Information Theory Workshop (2005, 2006, 2007, 2008, 2010)

Int. Conference on Performance Evaluation Methodologies & Tools (ValueTools 2006, 2007, 2008)

Information Theory and Statistical Learning Conference (2008)

INVITED SESSION ORGANIZER at various IEEE Information Theory Workshops and at the Conference on Information Sciences and Systems (CISS).

SEMINAR CO-CHAIR with Wojtek Szpankowski (Department of Computer Science, Purdue University) of the *Purdue Mini-Seminar on Analytic Information Theory*, hosted at Purdue University, April 1999.

SESSION CHAIR in numerous Conferences, including IEEE International Symposia on Information Theory, IEEE Information Theory Workshops, the Conference on Information Sciences and Systems (CISS).

SENIOR MEMBER of the Institute of Electrical and Electronic Engineers (IEEE)

MEMBER of the American Mathematical Society (AMS); Institute of Electrical and Electronic Engineers (IEEE) – Information Theory Society; Institute of Mathematical Statistics (IMS); London Mathematical Society (LMS); Mathematical Association of America (MAA); Society for Industrial and Applied Mathematics (SIAM).

REVIEWER of numerous manuscripts for:

- Over 30 leading international journals, published by the IEEE, ACM, IMS, AMS, SIAM, among others.
- Several books published by Springer-Verlag, the American Mathematical Society and other leading international publishers.
- Grant proposals for the National Science Foundation.
- Numerous international conferences.

TEACHING

CLASSES

Information Theory

Several undergraduate/graduate courses; introduction to information theory; channel coding and error-correcting codes, data compression, quantization, image/video compression algorithms, information theory and probability, communication networks

Stochastic Processes

Graduate course; non-measure theoretic; random walks, renewal theory, Markov processes in discrete and continuous time

Elementary Probability and Statistics

Undergraduate introduction to the fundamentals of probability and statistics for non-majors

Graduate Probability

Several graduate courses in measure-theoretic probability; measure theory, limit theorems, martingales, weak convergence, Brownian motion

Operations Research

Undergraduate/graduate course; optimization theory and algorithms, dynamic programming and probabilistic dynamic programming, Markov chain Monte Carlo methods, Markov decision problems, scheduling, applications in finance, business and simulation

GRADUATE STUDENTS

Principal advisor to one graduate student; co-advisor for two graduate students; member of the Ph.D. committee for eight graduate students

PERSONAL INFORMATION

Date/Place of Birth: January 24, 1972, Athens, Greece.

Nationality: Greek.

Updated September 18, 2010.

Daniel P. Palomar

Department of Electronic and Computer Engineering
Hong Kong University of Science and Technology
Clear Water Bay, Kowloon
Hong Kong

Phone: +852 2358 7060
Fax: +852 2358 1485
E-mail: palomar@ust.hk
URL: <http://www.ece.ust.hk/~palomar>

Academic Qualifications

Years	Institution	Qualification
1/1999 – 5/2003	Technical University of Catalonia (UPC), Barcelona, Spain (one year exchange at Stanford University)	Ph.D. cum laude in EE
1998	King's College London (KCL), London, UK	FYP with honors in EE
10/1993 – 10/1998	Technical University of Catalonia (UPC), Barcelona, Spain	B.Sc. with honors in EE

Summary of Employment

Period	Employment	Position
7/2010 – present	Hong Kong Univ. of Science and Technology (HKUST)	Associate Professor
8/2006 – 6/2010	Hong Kong Univ. of Science and Technology (HKUST)	Assistant Professor
3/2006 – 7/2006	Princeton University, Princeton, NJ	Research Associate
3/2004 – 2/2006	Princeton University, Princeton, NJ	Fulbright Research Fellow
11/2003 – 3/2004	University of Rome “La Sapienza”, Rome, Italy	Visiting Researcher
8/2003 – 11/2003	Royal Institute of Technology (KTH), Stockholm, Sweden	Guest Researcher
1/1999 – 8/2003	Technical University of Catalonia (UPC), Barcelona, Spain	Research Assistant
1/2002 – 12/2002	Telecomm. Tech. Center of Catalonia, Barcelona, Spain	Visiting Researcher
4/2001 – 11/2001	Stanford University, Stanford, CA	Visiting Researcher

Career Totals

Publications:	Books/monographs	2
	Book chapters	6
	Journal papers	43
	Conference papers	59
	h-index	14 (ISI Web of Knowledge) 22 (Google Scholar)
	Total citations	1,904 (Google Scholar)
	Highly cited paper	252 (ISI Web of Knowledge) 407 (Google Scholar)
	Funding:	Funded projects
Amount as PI		HK\$3,178,915
Students advised:	PhD/MPhil students	7
	Visiting students	5
	Postdocs	6

Honors and Awards

- Invited Instructor at the 2011 Winter School of Information Theory, Barcelona, Spain.
- Invited Speaker at the 2010 Workshop on Applications of Optimization in Science and Engineering, Institute for Pure and Applied Mathematics (IPAM), UCLA campus, LA, USA.
- Invited Speaker at the 2010 Workshop on Distributed Decision-Making and Control, LCCC, Lunds University, Sweden.
- **Keynote Speaker** at the 2009 Australian Communication Theory Workshop (AusCTW2009), University of New South Wales, Sydney, Australia.
- **Plenary Speaker** at the 2008 IEEE Workshop on Signal Proc. Advances in Wireless Comm. (SPAWC'08), Recife, Brazil.
- **Highly cited paper**¹ (ISI Web of Knowledge) status for my 2003 IEEE Trans. SP paper (coauthored by Lagunas and Cioffi) on majorization theory and convex optimization applied to MIMO transceiver design.
- Invited Speaker at the “Panel for Convex Optimization and Applications,” ICASSP 2008, Las Vegas, USA.
- Invited Speaker at the 2007 Workshop on Optimization and Signal Processing (WOSP), Hong Kong.
- Co-recipient of 2006 Best Student Paper Award at ICASSP'06, Toulouse, France.
- 2004 Young Author **Best Paper Award**² by the IEEE Signal Processing Society.
- 2004 Prize for the best Doctoral Thesis in Advanced Mobile Communications by the Vodafone Foundation and COIT.
- 3/2004 – 3/2006, Fulbright Scholarship at Princeton University, Princeton, NJ.
- 2002/2003 Rosina Ribalta first prize for the best Doctoral Thesis project within areas of Information Technologies and Communications by the Epson Foundation.
- 2002/2003 best Ph.D. prize within the area of Information Technologies and Communications by the Technical University of Catalonia (UPC).

Research Group

Current members:

Yifan Wang	PhD student	9/2010 – 7/2014
Yiyong Feng	PhD student	9/2010 – 7/2014
Francisco Rubio	Visiting Researcher	8/2010 – 9/2010
Frankie Chan	Postdoc	4/2010 – 3/2011
Yang Yang	MPhil student	9/2009 – 7/2013
Mengyi Zhang	PhD student	9/2009 – 7/2013
Jiaheng Wang	PhD student	9/2006 – 7/2010

Alumni:

Luxmiram Vijayandran	Visiting PhD student	2/2010 – 6/2010
Tian Wang	MPhil student	9/2008 – 7/2010
Luis García Ordóñez	Postdoc	10/2009 – 4/2010
Yongwei Huang	Postdoc	8/2009 – 3/2010
Javier Via	Visiting Professor	9/2009 – 1/2010
Gesualdo Scutari	Research Associate	2/2009 – 12/2009
Francisco Rubio	Visiting Researcher	8/2009 – 9/2009

¹ *Highly cited paper* is an official status given by the ISI Web of Science to the 1% top papers in terms of citations within the field according to Essential Science IndicatorsSM.

² The Young Author Best Paper Award is a very prestigious award given to an outstanding journal paper published by the IEEE Signal Society within a year (with the first author having no more than 30 years at the time of submission).

Francisco Rubio	Visiting Researcher	7/2008 – 8/2008
Gesualdo Scutari	Postdoc	5/2008 – 8/2008
Yongwei Huang	Postdoc	2/2008 – 4/2009
Svante Bergman	Visiting PhD student	2/2008 – 5/2008
Gesualdo Scutari	Postdoc	9/2007 – 1/2008
Luis G. Ordoñez	Visiting PhD student	3/2007 – 9/2007
Miquel Payaró	Postdoc	2/2007 – 12/2008
Jonathan Duplicy	Visiting PhD student	11/2006 – 4/2007
Xiaoting Wu	MPhil student	9/2006 – 12/2008

Visiting PhD students from Europe:

Luxmiram Vijayandran	Norwegian Univ. of Science and Technology (NTNU)	Advisor: Torbörn Ekman	Norway
Svante Bergman	Royal Institute of Technology (KTH)	Advisor: Björn Ottersten	Sweden
Luis G. Ordoñez	Technical Univ. of Catalonia (UPC)	Advisor: Javier R. Fonollosa	Spain
Jonathan Duplicy	Université catholique de Louvain (UCL)	Advisor: Luc Vandendorpe	Belgium

Funded Projects

Grant	Role	Title	Duration	Amount
RGC 2010/11-617810	PI	Variational Inequality Theory: A Framework for Optimization, Game Theory, and Complementary Problems with Applications in Signal Processing and Communication Systems	1/2011 – 12/2013	HK\$502,858
RGC 2009/10-618709	PI	Cognitive Radio Wireless Systems: From Conservative To Flexible Designs via Variational Inequalities	1/2010 – 12/2012	HK\$926,450
NSFC/RGC N_HKUST604/08	PI (joint w/Pingyin Fan)	Distributed Optimization of Infrastructureless MIMO Communication Networks via Game Theory	1/2009 – 12/2011	HK\$667,600
DAG_S08/09.EG05	PI	Precoder design for MIMO channels with arbitrary signaling	6/2009 – 6/2010	HK\$67,160
RGC09/10-610409	Partner (PI: Brahim Bensaou)	Joint Contention Windows adjustment and congestion control in multi-radio wireless mesh networks	7/2009 – 6/2012	HK\$658,007
Consolider-Ingenio project CDS2008-00010 (National Research Plan of Spain)	Partner (PI: Javier Fonollosa)	Foundations and Methodologies for Future Communication and Sensor Networks (COMONSENS)	2010 – 2015	€3,500,000
RGC08/09-618008	PI	Distribution of the Eigenvalues of Random Covariance Matrices with Applications to MIMO Communication Systems	1/2009 – 12/2010	HK\$571,647
HKTIT/VFP/08-003	PI	Fellow Visiting Program, to visit The Technion, Israel	12/2008 – 1/2009	HK\$43,200
RPC07/08.EG23	PI	Waveform Design for MIMO Radar: An Emerging and	5/2008 – 4/2010	HK\$300,000

		Promising Technology		
NSFC-60702081 (Mainland China)	Partner (PI: Weiqiang Xu)	Generalized Congestion Control for Ad Hoc Networks under the Non-cooperative and High Dynamic Environment	1/2008 – 12/2010	¥260,000
Consolider project TEC2006-06481/TCM (National Research Plan of Spain)	Partner (PI: Javier Fonollosa)	Fundamental Bounds in Network Information Theory (LITIS)	11/2006 – 11/2010	€360,000
DAG06/07.EG02	PI	Analytical Performance Characterization of Low- Complexity Linearly Precoded MIMO Systems	12/2006 – 11/2007	HK\$100,000

Professional Service

Journal Editorship

- Associate Editor of *IEEE Trans. on Signal Processing* (2007 – 2010).
- Editor of the book *Convex Optimization in Signal Processing and Communications*, Cambridge Univ. Press, 2009. (Co-editor: Yonina C. Eldar.)
- Guest Editor of the 2010 Special Issue of *IEEE Signal Processing Magazine* on “Convex Optimization for Signal Processing.” (Co-editors: T. Luo, Y. Eldar, K. Ma, and N. Sidiropoulos.)
- Guest Editor of the 2008 Special Issue of *IEEE Journal on Selected Areas in Communications* on “Game Theory in Communication Systems.” (Co-editors: J. Huang, N. Mandayan, S. Wicker, J. Walrand, and T. Basar.)
- Lead Guest Editor of the 2007 Special Issue of *IEEE Journal on Selected Areas in Communications* on “Optimization of MIMO Transceivers for Realistic Communication Network: Challenges and Opportunities.” (Co-editors: Tim Davidson, Sergio Barbarossa, Andrea Goldsmith, and Georgios Giannakis.)

Conference organization

- Chair of the IEEE Hong Kong Information Theory Society (2010).
- General Co-Chair of the 2009 IEEE Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP), Aruba.
- Member of the organizing committee (Tutorial Chair) of the 2015 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Brisbane, Australia.
- Member of the organizing committee (Tutorial Chair) of the 2011 European Signal Processing Conference (EUSIPCO), Barcelona, Spain. (pending of acceptance)
- Vice-Chair of the IEEE Hong Kong Information Theory Society (2009).
- Member of the organizing committee of the 2009 IEEE Workshop on Signal Proc. Advances in Wireless Comm. (SPAWC), Perugia, Italy.
- Member of the organizing committee of the 2009 IEEE Taiwan/Hong Kong/Macau Joint Workshop on Information Theory and Communications, Macau.
- Organizer of CAMSAP’09 special session on “Game Theory in Multisensor Signal Processing,” Aruba.
- Organizer of CIP2010 special session on “Game-theoretic tools for cognitive radios,” Elba, Italy.
- Organizer of GameNets’09 special session on “Game Theory for Communication Systems,” Istanbul, Turkey.
- Member of the IEEE SPCOM Technical Committee (2007 – 2009).
- Co-organizer of ICASSP-2007 special session on “Optimization of Communication Systems.” (Co-organizer: Mung Chiang.)

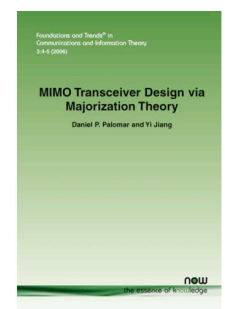
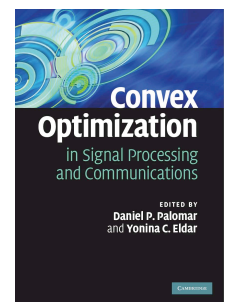
Review

- Member of the following Technical Program Committees (TPCs): CROWN 2010, Gamecomm 2009, GameNets 2009, ICCS 2008, ISIT 2009, Necsys 2009, RAWNET 2009, WiOpt 2009, CAMSAP 2009, SPAWC 2009, ICC 2009-2010, ISIT 2009, GameNets 2009, PIMRC 2008, ICASSP 2008, RAWNET 2008, WiOpt 2008, CAMSAP 2007, 2009, VTC 2007, WCNC 2007, RAWNET 2007, CAMSAP 2005, CAMSAP 2005.
- Reviewer for the following journals:
 - *IEEE Trans. on Signal Processing*
 - *IEEE Trans. on Information Theory*
 - *IEEE Trans. on Communications*
 - *IEEE Journal on Selected Areas in Communications*
 - *IEEE Trans. on Wireless Communications*
 - *IEEE Trans. on Automatic Control*
 - *IEEE Signal Processing Magazine*
 - *EURASIP Signal Processing*

Publications

Books and Monographs (2)

- Daniel P. Palomar and Yonina C. Eldar, Eds., *Convex Optimization in Signal Processing and Communications*, Cambridge University Press, 2009.
- Daniel P. Palomar and Yi Jiang, “MIMO Transceiver Design via Majorization Theory,” in *Foundations and Trends in Communications and Information Theory*, Now Publishers, vol. 3, no. 4-5, 2007.



Book Chapters (6)

- Gesualdo Scutari, Daniel P. Palomar, Francisco Facchinei, and Jong-Shi Pang, “Monotone Games for Cognitive Radio Systems,” in *Distributed Decision-Making and Control*, Eds. Anders Rantzer and Rolf Johansson, Lecture Notes in Control and Information Sciences Series, Springer Verlag, 2011.
- Jiaheng Wang and Daniel P. Palomar, “Majorization Theory with Applications in Signal Processing and Communication Systems,” in *Mathematical Foundations for Signal Processing, Communications and Networking*, Eds. Thomas Chen, Dinesh Rajan, and Erchin Serpedin, Cambridge University Press, 2011.
- Gesualdo Scutari, Daniel P. Palomar, and Sergio Barbarossa, “Competitive Optimization of Cognitive Radio MIMO Systems via Game Theory,” in *Convex Optimization in Signal Processing and Communications*, Eds. Daniel P. Palomar and Yonina C. Eldar, Cambridge University Press, 2009.

- Mung Chiang, Chee Wei Tan, Daniel P. Palomar, Daniel O'Neill, and David Julian, "Power Control by Geometric Programming," in *Resource Allocation in Next Generation Wireless Networks*, vol. 5, Chapter 13, pp. 289-313, W. Li, Y. Pan, Editors, Nova Sciences Publishers, ISBN 1-59554-583-9, 2005.
- Daniel P. Palomar, A. Pascual-Iserte, John M. Cioffi, and Miguel A. Lagunas, "Convex Optimization Theory Applied to Joint Transmitter-Receiver Design in MIMO Channels," in *Space-Time Processing for MIMO Communications*, Chapter 8, pp. 269-318, A. B. Gershman and N. Sidiropoulos, Editors, John Wiley & Sons, ISBN 0-470-01002-9, April 2005.
- Daniel P. Palomar, "Unified Design of Linear Transceivers for MIMO Channels," in *Smart Antennas – State-of-the-Art*, Chapter 18, EURASIP Hindawi Book Series, T. Kaiser, A. Bourdoux, H. Boche, J. R. Fonollosa, J. B. Andersen, and W. Utschick, Editors, ISBN 977-5945-09-7, 2005.

Journal Papers (43)

- Yongwei Huang and Daniel P. Palomar, "A Dual Perspective on Separable Semidefinite Programming with Applications to Optimal Downlink Beamforming," accepted in *IEEE Trans. on Signal Processing*, submitted Oct. 2009.
- Eduard Calvo, Daniel P. Palomar, Javier R. Fonollosa, and Josep Vidal, "On the Computation of the Capacity Region of the Discrete MAC," accepted in *IEEE Trans. On Communications*, submitted May 2009.
- Jiaheng Wang and Daniel P. Palomar, "Robust MSE Precoding in MIMO Channels with Pre-Fixed Receivers," accepted in *IEEE Trans. on Signal Processing*, submitted Aug. 2009.
- Jong-Shi Pang, Gesualdo Scutari, Daniel P. Palomar, and Francisco Facchinei, "Design of Cognitive Radio Systems Under Temperature-Interference Constraints: A Variational Inequality Approach," *IEEE Trans. on Signal Processing*, vol. 58, no. 6, pp. 3251-3271, June 2010.
- Gesualdo Scutari, Daniel P. Palomar, Francisco Facchinei, and Jong-Shi Pang, "Convex Optimization, Game Theory, and Variational Inequality Theory," *IEEE Signal Processing Magazine*, vol. 27, no. 3, pp. 35-49, May 2010.
- Gesualdo Scutari and Daniel P. Palomar, "MIMO Cognitive Radio: A Game Theoretical Approach," *IEEE Trans. on Signal Processing*, vol. 58, no. 2, pp. 761-780, Feb. 2010.
- Antonio De Maio, Silvio De Nicola, Yongwei Huang, Daniel P. Palomar, Shuzhong Zhang, and Alfonso Farina, "Code Design for Radar STAP via Optimization Theory," *IEEE Trans. on Signal Processing*, vol. 58, no. 2, pp. 679-694, Feb. 2010.
- Yongwei Huang and Daniel P. Palomar, "Rank-Constrained Separable Semidefinite Programming With Applications to Optimal Beamforming," *IEEE Trans. on Signal Processing*, vol. 58, no. 2, pp. 664-678, Feb. 2010.
- Svante Bergman, Daniel P. Palomar, and Björn Ottersten, "Joint Bit Allocation and Precoding for MIMO Systems with Decision Feedback Detection," *IEEE Trans. on Signal Processing*, vol. 57, no. 11, pp. 4509-4521, Nov. 2009.
- Gesualdo Scutari, Daniel P. Palomar, Jong-Shi Pang, and Francisco Facchinei, "Flexible Design for Cognitive Wireless Systems: From Game Theory to Variational Inequality Theory," *IEEE Signal Processing Magazine*, vol. 26, no. 5, pp. 107-123, Sept. 2009.
- Jiaheng Wang and Daniel P. Palomar, "Worst-Case Robust MIMO Transmission With Imperfect Channel Knowledge," *IEEE Trans. on Signal Processing*, vol. 57, no. 8, pp. 3086-3100, Aug. 2009.
- Miquel Payaró and Daniel P. Palomar, "Hessian and Concavity of Mutual Information, Differential Entropy, and Entropy Power in Linear Vector Gaussian Channels," *IEEE Trans. on Information Theory*, vol. 55, no. 8, pp. 3613-3628, Aug. 2009.
- Chee Wei Tan, Daniel P. Palomar, and Mung Chiang, "Energy-Robustness Tradeoff in Cellular Network Power Control," *IEEE/ACM Trans. on Networking*, vol. 17, no. 3, pp. 912-925, June 2009.
- Luis G. Ordóñez, Daniel P. Palomar, Alba Pagès-Zamora, and Javier R. Fonollosa, "Minimum BER Linear MIMO Transceivers with Adaptive Number of Substreams," *IEEE Trans. on Signal Processing*, vol. 57, no. 6, pp. 2336-2353, June 2009.

- Gesualdo Scutari, Daniel P. Palomar, and Sergio Barbarossa, “The MIMO Iterative Waterfilling Algorithm,” *IEEE Trans. on Signal Processing*, vol. 57, no. 5, pp. 1917-1935, May 2009.
- Luis G. Ordóñez, Daniel P. Palomar, and Javier R. Fonollosa, “Ordered Eigenvalues of a General Class of Hermitian Random Matrices With Application to the Performance Analysis of MIMO Systems,” *IEEE Trans. on Signal Processing*, vol. 57, no. 2, pp. 672-689, Feb. 2009.
- Gesualdo Scutari, Daniel P. Palomar, and Sergio Barbarossa, “Cognitive MIMO Radio: Competitive Optimality Design Based on Subspace Projections,” *IEEE Signal Processing Magazine*, vol. 25, no. 6, pp. 46-59, Nov. 2008.
- Gesualdo Scutari, Daniel P. Palomar, and Sergio Barbarossa, “Competitive Design of Multiuser MIMO Systems based on Game Theory: A Unified View,” *IEEE Journal on Selected Areas in Communications: Special Issue on Game Theory*, vol. 25, no. 7, pp. 1089-1103, Sept. 2008.
- Xi Zhang, Daniel P. Palomar, and Björn Ottersten, “Statistically Robust Design of Linear MIMO Transceivers,” *IEEE Trans. on Signal Processing*, vol. 56, no. 8, pp. 3678-3689, Aug. 2008.
- Gesualdo Scutari, Daniel P. Palomar, and Sergio Barbarossa, “Asynchronous Iterative Water-Filling for Gaussian Frequency-Selective Interference Channels,” *IEEE Trans. on Information Theory*, vol. 54, no. 7, pp. 2868-2878, July 2008.
- Daniel P. Palomar and Sergio Verdú, “Lautum Information,” *IEEE Trans. on Information Theory*, vol. 54, no. 3, pp. 964-975, March 2008.
- Gesualdo Scutari, Daniel P. Palomar, and Sergio Barbarossa, “Optimal Linear Precoding Strategies for Wideband Noncooperative Systems Based on Game Theory – Part I: Nash Equilibria,” *IEEE Trans. on Signal Processing*, vol. 56, no. 3, pp. 1230-1249, March 2008.
- Gesualdo Scutari, Daniel P. Palomar, and Sergio Barbarossa, “Optimal Linear Precoding Strategies for Wideband Noncooperative Systems Based on Game Theory – Part II: Algorithms,” *IEEE Trans. on Signal Processing*, vol. 56, no. 3, pp. 1250-1267, March 2008.
- Daniel P. Palomar and Mung Chiang, “Alternative Distributed Algorithms for Network Utility Maximization: Framework and Applications,” *IEEE Trans. on Automatic Control*, vol. 52, no. 12, pp. 2254-2269, Dec. 2007.
- Luis García-Ordóñez, Daniel P. Palomar, Alba Pagès-Zamora, and Javier R. Fonollosa, “High-SNR Analytical Performance of Spatial Multiplexing MIMO Systems with CSI,” *IEEE Trans. on Signal Processing*, vol. 55, no. 11, pp. 5447-5463, Nov. 2007.
- Mung Chiang, Chee Wei Tan, Daniel P. Palomar, Daniel O’Neill, and David Julian, “Power Control by Geometric Programming,” *IEEE Trans. on Wireless Communications*, vol. 6, no. 7, pp. 2640-2651, July 2007.
- Daniel P. Palomar and Sergio Verdú, “Representation of Mutual Information via Input Estimates,” *IEEE Trans. on Information Theory*, vol. 53, no. 2, pp. 453-470, Feb. 2007.
- Daniel P. Palomar and Mung Chiang, “A Tutorial on Decomposition Methods for Network Utility Maximization,” *IEEE Journal on Selected Areas in Communications: Special Issue on Nonlinear Optimization of Communication Systems*, vol. 24, no. 8, pp. 1439-1451, Aug. 2006.
- Daniel P. Palomar and Sergio Verdú, “Gradient of Mutual Information in Linear Vector Gaussian Channels,” *IEEE Trans. on Information Theory*, vol. 52, no. 1, pp. 141-154, Jan. 2006.
- A. Pascual-Iserte, Daniel P. Palomar, Ana I. Pérez-Neira, and Miguel A. Lagunas, “A Robust Maximin Approach for MIMO Communications with Partial Channel State Information Based on Convex Optimization,” *IEEE Trans. on Signal Processing*, vol. 54, no. 1, pp. 346-360, Jan. 2006.
- Daniel P. Palomar, “Convex Primal Decomposition for Multicarrier Linear MIMO Transceivers,” *IEEE Trans. on Signal Processing*, vol. 53, no. 12, pp. 4661-4674, Dec. 2005.
- Daniel P. Palomar and Sergio Barbarossa, “Designing MIMO Communication Systems: Constellation Choice and Linear Transceiver Design,” *IEEE Trans. on Signal Processing*, vol. 53, no. 10, pp. 3804-3818, Oct. 2005.
- Daniel P. Palomar, Mats Bengtsson, and Björn Ottersten, “Minimum BER Linear Transceivers for MIMO Channels via Primal Decomposition,” *IEEE Trans. on Signal Processing*, vol. 53, no. 8, pp. 2866-2882, Aug. 2005.

- Daniel P. Palomar and Javier Rodriguez Fonollosa, “Practical Algorithms for a Family of Waterfilling Solutions,” *IEEE Trans. on Signal Processing*, vol. 53, no. 2, pp. 686-695, Feb. 2005.
- Daniel P. Palomar, “Unified Framework for Linear MIMO Transceivers with Shaping Constraints,” *IEEE Communications Letters*, vol. 8, no. 12, pp. 697-699, Dec. 2004.
- Daniel P. Palomar, Miguel Angel Lagunas, and John M. Cioffi, “Optimum Linear Joint Transmit-Receive Processing for MIMO Channels with QoS Constraints,” *IEEE Trans. on Signal Processing*, vol. 52, no. 5, pp. 1179-1197, May 2004.
- Daniel P. Palomar, John M. Cioffi, and Miguel Angel Lagunas, “Joint Tx-Rx Beamforming Design for Multicarrier MIMO Channels: A Unified Framework for Convex Optimization,” *IEEE Trans. on Signal Processing*, vol. 51, no. 9, pp. 2381-2401, Sept. 2003.
 - ↳ 🏆 2004 Young Author **Best Paper Award** by the IEEE Signal Processing Society
 - ↳ 📖 **Highly cited paper** (ISI Web of Knowledge)
- Daniel P. Palomar, John M. Cioffi, and Miguel Angel Lagunas, “Uniform Power Allocation in MIMO Channels: A Game-Theoretic Approach,” *IEEE Trans. on Information Theory*, vol. 49, no. 7, pp. 1707-1727, July 2003.
- Daniel P. Palomar and Miguel Angel Lagunas, “Joint Transmit-Receive Space-Time Equalization in Spatially Correlated MIMO channels: A Beamforming Approach,” *IEEE Journal on Selected Areas in Communications: Special Issue on MIMO Systems and Applications*, vol. 21, no. 5, pp. 730-743, June 2003.
- Daniel P. Palomar and Miguel Angel Lagunas, “Temporal diversity on DS-CDMA communication systems for blind array signal processing,” *EURASIP Signal Processing*, vol. 81, no. 8, pp. 1625-1640, Aug. 2001.
- Daniel P. Palomar, Montse Najar, and Miguel Angel Lagunas, “Self-reference Spatial Diversity Processing for Spread Spectrum Communications,” *AEÜ International Journal of Electronics and Communications*, vol. 54, no. 5, pp. 267-276, Nov. 2000.
- Daniel P. Palomar, Marc Price, and Mark Sandler, “Re-optimization of LPC filters for multi-pulse coded excitation,” *IEE Electronics Letters*, vol. 35, N. 13, pp. 1058-1059, ISSN 0013-5194, June 1999.
- Daniel P. Palomar, “Implementación de filtros digitales en tiempo real,” (in Spanish), *Sólo Programadores*, 1997.

Conference Papers

See appendix.

Ph.D. Dissertation

- Daniel P. Palomar, “A Unified Framework for Communications through MIMO Channels,” Ph.D. dissertation, Technical University of Catalonia (UPC), Barcelona, Spain, May 27, 2003.

Electrical Engineering Degree Thesis

- Daniel P. Palomar, “Coding of the Residual-LPC Analysis for High Quality Speech Compression,” Electrical Engineering Degree Thesis, King's College London (supervised by Prof. Mark Sandler) and Technical University of Catalonia (UPC), July 1998.

Invited Talks and Seminars

- March 12, 2010, Invited Talk “Design of Cognitive Radio Systems Under Temperature-Interference Constraints: A Variational Inequality Approach,” Workshop on Distributed Decision-Making and Control, LCCC, Lunds University, Sweden.
- January 22, 2010, “Primal and Dual Perspectives of Rank-Constrained Semidefinite Programming with Applications to Optimal Beamforming,” Dept. IESE, Univ. of Illinois at Urbana-Champaign (UIUC), IL, USA.

- January 22, 2010, “Rank-Constrained Separable Semidefinite Programming with Applications to Optimal Beamforming,” Dept. ECE, Univ. of Illinois at Urbana-Champaign (UIUC), IL, USA.
- June 27, 2009, “Rank-Constrained Separable Semidefinite Programming with Applications to Optimal Beamforming,” Distinguished Seminar Series, Yonsei University, Seoul, Korea.
- June 18, 2009, “Rank-Constrained Separable Semidefinite Programming with Applications to Optimal Beamforming,” Università di Pisa, Pisa, Italy. (in Italian)
- June 16, 2009, “Rank-Constrained Separable Semidefinite Programming with Applications to Optimal Beamforming,” Università degli Studi di Napoli “Federico II”, Napoli, Italy. (in Italian)
- June 15, 2009, “Rank-Constrained Separable Semidefinite Programming with Applications to Optimal Beamforming,” University of Rome “La Sapienza”, Rome, Italy. (in Italian)
- April 20, 2009, Tutorial at ICASSP’09 “A Unified Design Framework for Non-Linear MIMO Transceivers Using Majorization Theory,” Taipei, Taiwan. (Co-lectured with Michael Botros Shenouda and Tim Davidson.)
- April 11, 2009, Invited Talk “Connections Between Information Theory and Estimation Theory in the Vector Case,” Princeton University, Princeton, NJ, USA.
- February 6, 2009, **Keynote Talk** “MIMO Transceiver Design: from Signal Processing to Information Theory,” Australian Communication Theory Workshop (AusCTW2009), New South Wales, Australia.
- December 19-21, 2008, 18-hour Course on “Convex Optimization for Wireless Communications and Signal Processing,” National Chiao Tung Univ., Hsinchu, Taiwan. (Co-taught with Ken Ma.)
- July 8, 2008, **Plenary Talk** “MIMO Transceiver Design: from Signal Processing to Information Theory,” IEEE Workshop on Signal Proc. Advances in Wireless Comm. (SPAWC).
- June 19, 2008, “MIMO Transceiver Design: from Signal Processing to Information Theory,” ECE Seminar, HKUST, Hong Kong.
- January 28, 2008, “Decision-Feedback MIMO Transceiver Design via Majorization Theory,” Workshop on Information Theory and Applications (ITA), UCSD, San Diego, CA, USA.
- January 24, 2008, “MIMO Transceiver Design via Majorization Theory: From Linear to DF Schemes,” ISS Seminar, Princeton University, Princeton, NJ, USA.
- January 23, 2008, “MIMO Transceiver Design via Majorization Theory: From Linear to DF Schemes,” Winlab, Rutgers University, New Brunswick, NJ, USA.
- December 19, 2007, “MIMO Transceiver Design via Majorization Theory,” Workshop on Optimization and Signal Processing, CUHK, Hong Kong.
- January 22, 2007, “Waterfillings, Waterfillings, and Waterfillings: From Single-User to Multiuser,” ISS Seminar, Princeton University, Princeton, NJ, USA.
- January 19, 2007, “Waterfillings, Waterfillings, and Waterfillings: From Single-User to Multiuser,” Columbia University, New York City, NY, USA.
- January 18, 2007, “Waterfillings, Waterfillings, and Waterfillings: From Single-User to Multiuser,” Winlab, Rutgers University, New Brunswick, NJ, USA.
- April 12, 2006, “Design of MIMO Communication Systems: A Marriage of Majorization Theory and Convex Optimization Theory,” University of California – Los Angeles, Los Angeles, CA, USA.
- March 28, 2006, “Design of MIMO Communication Systems: A Marriage of Majorization Theory and Convex Optimization Theory,” Ohio State University, Columbus, OH, USA.
- March 23, 2006, “Design of Wireless MIMO Systems: A Marriage of Majorization Theory and Convex Optimization Theory,” Washington University in St. Louis, St. Louis, MO, USA.
- March 13, 2006, “Linear Transceivers for MIMO Channels: A Marriage of Majorization Theory and Convex Optimization Theory,” University of Delaware, Newark, DE, USA.
- March 8, 2006, “Signal Processing for MIMO Communication Systems: A Marriage of Majorization Theory and Convex Optimization Theory,” University of Wisconsin-Madison, MA, USA.
- March 6, 2006, “Connections Between Information Theory and Estimation Theory,” Queen’s University, Kingston, Ontario, Canada.

- February 24, 2006, “Signal Processing for MIMO Channels: A Marriage of Majorization Theory and Convex Optimization Theory,” University of Connecticut, Storrs, CT, USA.
- February 3, 2006, “Linear Transceivers for MIMO Channels: A Marriage of Majorization Theory and Convex Optimization Theory,” Drexel University, Philadelphia, PA, USA.
- January 20, 2006, “Signal Processing for MIMO Channels: A Marriage of Majorization Theory and Convex Optimization Theory,” Hong Kong University of Science and Technology (HKUST), Hong Kong, China.
- November 14, 2005, “Design of Linear Transceivers for MIMO Channels: A Unified Framework for Convex Optimization,” Winlab, Rutgers University, New Brunswick, NJ, USA.
- November 1, 2005, “Design of Linear Transceivers for MIMO Channels: A Unified Framework for Convex Optimization,” Bell Labs, Lucent Technologies, Holmdel, NJ, USA.
- October 6, 2005, “Design of Linear Transceivers for MIMO Channels: A Unified Framework for Convex Optimization,” ISS Seminar, Princeton University, Princeton, NJ, USA.
- March 5, 2004, “Minimum BER Linear Transceivers for MIMO Channels via Primal Decomposition,” Dept. of Signal Theory and Communications, Technical University of Catalonia (UPC), Barcelona, Spain.
- December 5, 2003, “A Unified Framework for Linear Transceiver Design in MIMO Communication Systems,” INFOCOM Department, University of Rome “La Sapienza”, Rome, Italy.
- November 17-19, 2003, “A Primer on Convex Optimization Theory,” as part of a Ph.D. course, Dept. of Signal Theory and Communications, Technical University of Catalonia (UPC), Barcelona, Spain.
- November 11, 2003, “Minimum BER Linear Transceivers for MIMO Channels,” Dept. of Signals, Sensors & Systems, Royal Institute of Technology (KTH), Stockholm, Sweden.
- October 22, 2003, “A Unified Framework to Design Linear Transceivers for Communications through MIMO Channels,” Ericsson, Stockholm, Sweden.
- August 28, 2003, “A Unified Framework for Communications through MIMO Channels,” Dept. of Signals, Sensors & Systems, Royal Institute of Technology (KTH), Stockholm, Sweden.
- October 30, 2002, “Optimum Joint Transmit-Receive Linear Processing for Vektored DSL Transmission with QoS Requirements,” Dept. of Electrical Engineering, Stanford University, Stanford, CA, USA.

Appendix: Conference Papers

Conference Papers – 2010

- Luis G. Ordóñez, Daniel P. Palomar, and Javier R. Fonollosa, “On the Diversity, Multiplexing, and Array Gain Tradeoff in MIMO Channels,” in *Proc. IEEE International Symposium on Information Theory (ISIT'10)*, Austin, TX, USA, June 13-18, 2010.
- Ronit Bustin, Miquel Payaró, Daniel P. Palomar, and Shlomo Shamai, “On MMSE Properties and I-MMSE Implications in Parallel MIMO Gaussian Channels,” in *Proc. IEEE International Symposium on Information Theory (ISIT'10)*, Austin, TX, USA, June 13-18, 2010.
- Jiaheng Wang, Gesualdo Scutari, and Daniel P. Palomar, “Robust Cognitive Radio via Game Theory,” in *Proc. IEEE International Symposium on Information Theory (ISIT'10)*, Austin, TX, USA, June 13-18, 2010.
- Yongwei Huang and Daniel P. Palomar, “A Dual Perspective on Separable Semidefinite Programming with Applications to Optimal Beamforming,” in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Dallas, TX, USA, March 14-19, 2010.
- Jong-Shi Pang, Gesualdo Scutari, Daniel P. Palomar, and Francisco Facchinei, “Design of Cognitive Radio Systems Under Temperature-Interference Constraints: A Variational Inequality Approach,” in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Dallas, TX, USA, March 14-19, 2010.

Conference Papers – 2009

- Yongwei Huang and Daniel P. Palomar, “Rank-Constrained Separable Semidefinite Programming for Optimal Beamforming Design,” in *Proc. IEEE International Symposium on Information Theory (ISIT'09)*, Seoul, Korea, June 28 - July 3, 2009.
- Miquel Payaró and Daniel P. Palomar, “On optimal precoding in linear vector Gaussian channels with arbitrary input distribution,” in *Proc. IEEE International Symposium on Information Theory (ISIT'09)*, Seoul, Korea, June 28 - July 3, 2009.
- Gesualdo Scutari, Daniel P. Palomar, and Sergio Barbarossa, “Competitive Optimization of Cognitive Radio MIMO Systems via Game Theory,” in *Proc. International Conference on Game Theory for Networks (GameNets 2009)*, Boğaziçi University, Istanbul, Turkey, May 13-15, 2009.
- Svante Bergman, Daniel P. Palomar, and Björn Ottersten, “Optimal Bit Loading for MIMO Systems with Decision Feedback Detection,” in *Proc. IEEE Vehicular Technology Conference (VTC2009-Spring)*, Barcelona, Spain, April 26-29, 2009.
- Jiaheng Wang and Daniel P. Palomar, “Maximin Robust Design for MIMO Communication Systems Against Imperfect CSIT,” in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Taipei, Taiwan, April 19-24, 2009.

Conference Papers – 2008

- Are Hjørungnes and Daniel P. Palomar, “Finding Patterned Complex-Valued Matrix Derivatives by Using Manifolds,” in *Proc. IEEE First Symposium on Applied Sciences in Biomedical and Communication Technologies, (ISABEL 2008)*, Aalborg, Denmark, Oct. 2008.
- Are Hjørungnes and Daniel P. Palomar, “Patterned Complex-Valued Matrix Derivatives,” in *Proc. IEEE Sensor Array and Multichannel Signal Processing Workshop (SAM)*, Darmstadt, Germany, July 21-23, 2008.
- Eduard Calvo, Daniel P. Palomar, Javier R. Fonollosa, and Josep Vidal, “The Computation of the Capacity Region of the Discrete Degraded BC is a Nonconvex DC Problem,” in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Toronto, Canada, July 6-11, 2008.
- Miquel Payaró and Daniel P. Palomar, “A Multivariate Generalization of Costa’s Entropy Power Inequality,” in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Toronto, Canada, July 6-11, 2008.

- Gesualdo Scutari, Daniel P. Palomar, and Sergio Barbarossa, “MIMO Cognitive Radio: A Game-Theoretical Approach,” in *Proc. 9th IEEE Workshop on Signal Processing Advances in Wireless Communications (SPAWC 2008)*, Recife, Brazil, July 7-9, 2008.
- Luis García-Ordoñez, Daniel P. Palomar, and Javier R. Fonollosa, “Ordered Eigenvalues of a General Class of Hermitian Random Matrices and Performance Analysis of MIMO Systems,” in *Proc. IEEE 2008 International Conference on Communications (ICC’03)*, Beijing, China, May 19-23, 2008.
- Gesualdo Scutari, Daniel P. Palomar, and Sergio Barbarossa, “Competitive Design of Multiuser MIMO Interference Systems Based on Game Theory: A Unified Framework,” in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Las Vegas, NV, USA, March 30-April 4, 2008.

Conference Papers – 2007

- Jonathan Duplity, Daniel P. Palomar, and Luc Vandendorpe, “Adaptive Orthogonal Beamforming for the MIMO Broadcast Channel,” in *Proc. Second International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP 2007)*, St. Thomas, Virgin Islands, USA, Dec. 12-14, 2007.
- Gesualdo Scutari, Daniel P. Palomar, and Sergio Barbarossa, “Optimal Decentralized Linear Precoding for Wideband Non-Cooperative Interference Systems Based on Game Theory,” in *Proc. Second International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP 2007)*, St. Thomas, Virgin Islands, USA, Dec. 12-14, 2007.
- Yi Jiang, Mahesh K. Varanasi, and Daniel P. Palomar, “Decision Feedback Based Transceiver Optimization for MIMO Intersymbol Interference Channels,” in *Proc. 41st Asilomar Conference on Signals, Systems & Computers*, Pacific Grove, CA, USA, Nov. 4-7, 2007.
- Xi Zhang, Daniel P. Palomar, and Björn Ottersten, “Robust MAC MIMO Transceiver Design with Partial CSIT and CSIR,” in *Proc. 41st Asilomar Conference on Signals, Systems & Computers*, Pacific Grove, CA, USA, Nov. 4-7, 2007.
- Eduard Calvo, Daniel P. Palomar, Javier R. Fonollosa, and Josep Vidal, “The Computation of the Capacity Region of the Discrete MAC is a Rank-One Non-Convex Optimization Problem,” in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Nice, France, June 24-29, 2007.
- Chee Wei Tan, Daniel P. Palomar, and Mung Chiang, “Exploiting Hidden Convexity for Flexible and Robust Resource Allocation in Cellular Networks,” in *Proc. IEEE Infocom*, Anchorage, Alaska, USA, May 6-12, 2007.
- Luis G. Ordoñez, Daniel P. Palomar, Alba Pagès-Zamora, and Javier R. Fonollosa, “On Equal Constellation Minimum BER Linear MIMO Transceivers,” in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Honolulu, Hawaii, USA, April 15-20, 2007.
- Are Hjørungnes, David Gesbert, and Daniel P. Palomar, “Unified Theory of Complex-Valued Matrix Differentiation,” in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Honolulu, Hawaii, USA, April 15-20, 2007.
- Gesualdo Scutari, Daniel P. Palomar, and Sergio Barbarossa, “Distributed Totally Asynchronous Iterative Waterfilling for Wideband Interference Channel with Time/Frequency Offset,” in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Honolulu, Hawaii, USA, April 15-20, 2007.
- Yi Jiang, Daniel P. Palomar, and Mahesh K. Varanasi, “Precoder Optimization for Nonlinear MIMO Transceiver Based on Arbitrary Cost Function,” in *Proc. Conference on Information Sciences and Systems (CISS 2007)*, The John Hopkins University, Baltimore, MD, March 14-16, 2007.
- Gesualdo Scutari, Daniel P. Palomar, and Sergio Barbarossa, “Asynchronous Iterative Waterfilling for Gaussian Frequency-Selective Interference Channels: A Unified Framework,” in *Proc. Information Theory and Applications (ITA) Workshop*, San Diego, CA, USA, Jan. 29 - Feb. 2, 2007.

Conference Papers – 2006

- Gesualdo Scutari, Daniel P. Palomar, and Sergio Barbarossa, “Simultaneous Iterative Water-Filling for Gaussian Frequency-Selective Interference Channels,” in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Seattle, WA, USA, July 9-14, 2006.
- Gesualdo Scutari, Daniel P. Palomar, and Sergio Barbarossa, “Asynchronous Iterative Water-Filling for Gaussian Frequency-Selective Interference Channels: A Unified Framework,” in *Proc. IEEE Workshop on Signal Proc. Advances in Wireless Commun. (SPAWC 2006)*, Cannes, France, July 2-5, 2006.
- Xi Zhang, Daniel P. Palomar, and Björn Ottersten, “Robust Design of Linear MIMO Transceivers under Channel Uncertainty,” in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Toulouse, France, May 14-19, 2006.
- Gesualdo Scutari, Sergio Barbarossa, and Daniel P. Palomar, “Potential Games: A Framework for Vector Power Control Problems with Coupled Constraints,” in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Toulouse, France, May 14-19, 2006.

☺ **Best Student Paper Award at ICASSP**

- Chee Wei Tan, Daniel P. Palomar, and Mung Chiang, “Distributed Optimization of Coupled Systems with Applications to Network Utility Maximization,” in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Toulouse, France, May 14-19, 2006.
- Daniel P. Palomar and Mung Chiang, “Alternative Decompositions for Distributed Maximization of Network Utility: Framework and Applications,” in *Proc. IEEE Infocom*, Barcelona, Spain, April 23-29, 2006.
- Daniel P. Palomar and Sergio Verdú, “Lautum Information,” in *Proc. IEEE Information Theory Workshop (ITW)*, Punta del Este, Uruguay, March 13-17, 2006.

Conference Papers – 2005

- Daniel P. Palomar and Mung Chiang, “Alternative Decompositions and Distributed Algorithms for Network Utility Maximization,” in *Proc. Globecom*, St. Louis, MO, USA, Nov. 28 – Dec. 2, 2005.
- Chee Wei Tan, Daniel P. Palomar, and Mung Chiang, “Solving Nonconvex Power Control Problems in Wireless Networks: Low SIR Regime and Distributed Algorithms,” in *Proc. Globecom*, St. Louis, MO, USA, Nov. 28 – Dec. 2, 2005.
- Xi Zhang, Daniel P. Palomar, and Björn Ottersten, “Robust Design of Linear MIMO Transceivers for Low SNR,” in *Proc. 39th Asilomar Conference on Signals, Systems & Computers*, Pacific Grove, CA, USA, Oct. 30 - Nov. 2, 2005.
- Daniel P. Palomar and Sergio Verdú, “Estimation-Theoretic Representation of Mutual Information,” in *Proc. 43th Annual Allerton Conference on Communication, Control, and Computing*, Allerton House, Monticello, IL, USA, Sept. 28-30, 2005.
- Daniel P. Palomar and Sergio Verdú, “Gradient of Mutual Information in Linear Vector Gaussian Channels,” in *Proc. IEEE 2005 International Symposium on Information Theory (ISIT’05)*, Adelaide, Australia, Sept. 4-9, 2005.
- Luis García-Ordoñez, Daniel P. Palomar, Alba Pagès-Zamora, and Javier R. Fonollosa, “Analytical BER Performance in Spatial Multiplexing MIMO Systems,” in *Proc. IEEE Workshop on Signal Proc. Advances in Wireless Commun. (SPAWC 2005)*, New York, USA, June 5-8, 2005.

Conference Papers – 2004

- Daniel P. Palomar, Adrian Agustín, Olga Muñoz, and Josep Vidal, “Decode-and-Forward Protocol for Cooperative Diversity in Multi-Antenna Wireless Networks,” in *Proc. Conference on Information Sciences and Systems (CISS 2004)*, Princeton University, Princeton, NJ, March 17-19, 2004.

Conference Papers – 2003

- Diego Bartolomé, Daniel P. Palomar, and Ana I. Pérez-Neira, “Real-Time Scheduling for Wireless Multiuser MISO Systems under different Fairness Criteria,” in *Proc. IEEE Seventh International Symposium on Signal Processing and its Applications (ISSPA’03)*, Paris, France, July 1-4, 2003.

- Daniel P. Palomar, John M. Cioffi, and Miguel Angel Lagunas, “Uniform Power Allocation in MIMO Channels: A Game-Theoretic Approach,” in *Proc. IEEE 2003 International Symposium on Information Theory (ISIT’03)*, p. 271, Pacifico, Yokohama, Japan, June 29-July 4, 2003.
- Daniel P. Palomar, John M. Cioffi, Miguel Angel Lagunas, and Antonio Pascual, “Convex Optimization Theory Applied to Joint Beamforming Design in Multicarrier MIMO Channels,” in *Proc. IEEE 2003 International Conference on Communications (ICC’03)*, vol. 4, pp. 2974-2978, Anchorage, AK, May 11-15, 2003.

Conference Papers – 2002

- Daniel P. Palomar, Miguel Angel Lagunas, and John M. Cioffi, “On the Optimal Structure of Transmit-Receive Linear Processing for MIMO Channels,” in *Proc. 40th Annual Allerton Conference on Communication, Control, and Computing*, pp. 683-692, Allerton House, Monticello, IL, Oct. 2-4, 2002.
- Daniel P. Palomar, Miguel Angel Lagunas, and John M. Cioffi, “Optimum Joint Transmit-Receive Linear Processing for Vectored DSL Transmission with QoS Requirements,” in *Proc. 36th Asilomar Conference on Signals, Systems & Computers*, pp. 388-392, Pacific Grove, CA, Nov. 3-6, 2002.
- Antonio Pascual Iserte, Ana I. Pérez-Neira, Daniel P. Palomar, and Miguel Angel Lagunas, “Power Allocation Techniques for Joint Beamforming in OFDM-MIMO Channels,” in *Proc. XI European Signal Processing Conference (EUSIPCO 2002)*, Toulouse, France, Sept. 3-6, 2002.

Conference Papers – 2001

- Daniel P. Palomar and Miguel Angel Lagunas, “Capacity of spatially flattened frequency-selective MIMO channels using linear processing techniques in transmission,” in *Proc. 35th IEEE Annual Conference on Information Sciences and Systems (CISS 2001)*, The John Hopkins University, Baltimore, MD, March 21-23, 2001.
- Daniel P. Palomar, Javier R. Fonollosa, and Miguel Angel Lagunas, “Capacity results of spatially correlated frequency-selective MIMO channels in UMTS,” in *Proc. IEEE Vehicular Technology Conf. Fall (VTC-Fall 2001)*, Atlantic City, NJ, Oct. 7-11, 2001.
- Daniel P. Palomar, Miguel Angel Lagunas, Antonio Pascual, and Ana Pérez Neira, “Practical implementation of jointly designed transmit-receive space-time IIR filters,” in *Proc. 6th IEEE International Symposium on Signal Processing and its Applications (ISSPA-2001)*, pp. 521-524, Kuala-Lumpur, Malaysia, Aug. 13-16, 2001.
- Daniel P. Palomar, Javier R. Fonollosa, and Miguel Angel Lagunas, “Information-theoretic results for realistic UMTS MIMO channels,” in *Proc. IST Mobile Communication Summit*, Sitges, Barcelona, Spain, Sept. 9-12, 2001.

Conference Papers – 2000

- Daniel P. Palomar, Javier R. Fonollosa, and Miguel Angel Lagunas, “Capacity results on frequency-selective Rayleigh MIMO channels,” in *Proc. IST Mobile Comm. SUMMIT 2000*, pp. 491-496, Galway, Ireland, Oct. 1-4, 2000.
- Daniel P. Palomar, Javier R. Fonollosa, and Miguel Angel Lagunas, “MMSE Joint Detection in frequency-selective wireless communication channels for DS-CDMA systems,” in *Proc. IEEE Sixth International Symposium on Spread Spectrum Techniques & Applications (ISSSTA 2000)*, vol. 2, pp. 530-534, Parsippany, NJ, Sept. 6-8, 2000.
- Daniel P. Palomar and Miguel Angel Lagunas, “Optimum Self-reference Spatial Diversity Processing for FDSS and FH communication systems,” in *Proc. EUSIPCO 2000*, vol. III, Tampere, Finland, Sept. 4-8, 2000.
- Miguel Angel Lagunas, Daniel P. Palomar, and Ana I. Pérez Neira, “Diversidad espacio/tiempo en transmisión-recepción para comunicaciones móviles,” (in Spanish), *URSI-2000*, Zaragoza, Spain, Sept. 2000.
- Daniel P. Palomar and Miguel Angel Lagunas, “Self-reference beamforming for DS-CDMA communication systems,” in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP2000)*, vol. V, pp.3001-3004, Istanbul, Turkey, June 5-9, 2000.

- Daniel P. Palomar, Miguel Angel Lagunas, and Montse Nájjar, “Self-reference Spatial Diversity Processing for Spread Spectrum Communications,” in *Proc. of International Symposium on Image/Video Communications over Fixed and Mobile Networks (ISIVC'2000)*, Invited Presentation, vol. 1, pp. 81-96, Rabat, Morocco, April 17-20, 2000.

Conference Papers – 1999

- Daniel P. Palomar and Miguel Angel Lagunas, “Blind beamforming for DS-CDMA systems,” in *Proc. of the Fifth Bayona Workshop on Emerging Technologies in Telecommunications*, pp. 83-87, Bayona, Spain, Sept. 6-8, 1999.

Biography

Antonia M. Tulino (M'00–SM'05) received the Ph.D. degree from the Electrical Engineering Department, Seconda Università degli Studi di Napoli, Italy, in 1999.

She has served as Associate Professor at the Department of Electrical and Telecommunications Engineering at the Università degli Studi di Napoli “Federico II” since 2002. She is currently with the Department of Wireless Communications, Bell Laboratories, Alcatel-Lucent, Holmdel, NJ. She held research positions at the Center for Wireless Communications, Oulu, Finland and at the Department of Electrical Engineering, Princeton University, Princeton, NJ. She has served on the Faculty of Engineering, Università degli Studi del Sannio, Benevento, Italy. Dr. Tulino has received the 2009 Stephen O. Rice Prize in the Field of Communications Theory for the best paper published in the IEEE TRANSACTION ON COMMUNICATIONS in 2008. A frequent contributor to the IEEE TRANSACTIONS ON INFORMATION THEORY, the IEEE TRANSACTIONS ON COMMUNICATIONS, and the IEEE TRANSACTIONS ON SIGNAL PROCESSING, her research interests lay in the broad area of communication systems approached with the complementary tools provided by signal processing, information theory, and random matrix theory.

Publication List

MONOGRAPH

- M1 A. M. Tulino and S. Verdú, "Random Matrices and Wireless Communications," Now Publishers, Hanover, MA 2004, ISBN: 193301900-X.

BOOK CHAPTERS

- B1 A. M. Tulino, A. Lozano, S. Verdú, "Bandwidth- Power Tradeoff of Multi-antenna Systems in the Low-Power Regime", *Multiantenna channels: Capacity, Coding and Signal Processing*, G. Foschini and S. Verdú, Eds., DIMACS Series in Discrete Mathematics and Theoretical Computer Sciences, vol. 62, pp. 15-42, American Mathematical Society Press, 2003.
- B2 A. Lozano, A. M. Tulino, S. Verdú, "Multiantenna Capacity: Myths and Realities", Chapter 8, *Space-Time Wireless Systems: From Array Processing to MIMO Communications* H. Boelcskei, D. Gesbert, C. Papadias, and A. J. van der Veen,, Eds., Cambridge University Press, 2006.
- B3 J. G. Andrews, I. Collings, R. W. Heath, M. McKay, A. Tulino, "Joint Detection for Multi-Antenna Channels", M. L. Honig (Ed.), "Advances in Multiuser Detection", J. Wiley & Sons, Inc, to be published, 2008.
- B4 A..M. Tulino "The eta and Shannon transforms: A bridge between random matrices & wireless communications ",Random Matrix Theory and its Applications, Lecture Notes Series, Institute for Mathematical Sciences, National University of Singapore **18**, World Scientific, Singapore, 2009.
- B5 A. M. Tulino and S. Verdù, "Asymptotic Singular Value Distributions in Information Theory", Handbook of Random Matrix Theory, Oxford University Press,2010.

JOURNAL PAPERS

- J36 G. Alfano, A. Demaio, A. M. Tulino, "A theoretical framework for LMS MIMO communication systems performance analysis", to appear on *Transaction on Information Theory* 2010.
- J35 A. Aubry, M. Lops, A. M. Tulino, L. Venturino, "Statistical MIMO Radar under non-Gaussian target scattering", to appear on *Transaction on Information Theory* 2010.
- J34 A. Tulino, G. Caire and S. Shamai (Shitz), S. Verdu, "Capacity of Channels with Frequency-Selective and Time-Selective Fading,"*IEEE Transaction on Information Theory*, Vol.56, no., pp. 349-410, March 2010.
- J33 M.R McKay, I. B. Collings, and A. M. Tulino, "Achievable Sum Rate of MIMO MMSE Receivers: A General Analytic Framework", *IEEE Transaction on Information Theory*, Vol.56, no., pp. 349-410, January 2010.

- J32 M. Paturzo, P. Memmolo, A. Tulino, A. Finizio, and P. Ferraro, "Investigation of angular multiplexing and de-multiplexing of digital holograms recorded in microscope configuration", *Opt. Express* 17, 8709-8718 (2009).
- J31 M. Paturzo, P. Memmolo, L. Miccio, A. Finizio, P. Ferraro, A. Tulino, B. Javidi, "Numerical multiplexing and demultiplexing of digital holographic information for remote reconstruction in amplitude and phase" *Optics Letters*. 33, 2629-2631 (2008).
- J30 A. Lozano, A. M. Tulino and S. Verdú, "Optimum Power Allocation for Multiuser OFDM with Arbitrary Signal Constellations", *IEEE Transactions on Communications*, vol. 56, no. 5, pp. 828-837, May, 2008
- J29 G. Bacci, M. Luise, H. V. Poor and A.M. Tulino, "Energy-Efficient Power Control in Impulse Radio UWB Wireless Networks", *Journal on Selected Areas in Communications (Special Issue on Performance Limits of Ultra-Wideband Systems)*, vol. 1, no. 3, pp. 508-521, Oct. 2007.
- J28 A. M. Tulino and S. Verdú,, "Monotonic Decrease of the Non-Gaussianness of the Sum of Independent Random Variables: A Simple Proof" *IEEE Transaction on Information Theory*, vol. 52, no. 9, pp. 4295-4297, Sep. 2006.
- J27 A. Lozano, A. M. Tulino and S. Verdú,, "Optimum Power Allocation for Parallel Gaussian Channels with Arbitrary Input Distributions," *IEEE Transaction on Information Theory*, vol. 52, no.7, pp. 3033-3051, July 2006.
- J26 A. Lozano, A. M. Tulino, and S. Verdú "Capacity-Achieving Input Covariance for Single-User Multi-Antenna Channels," *IEEE Trans. on Wireless Communication*, vol. 5, no. 3, pp. 662-671, Mar. 2006.
- J25 A. Lozano, A. M. Tulino, and S. Verdú, "High-SNR Power Offset in Multiantenna Communication," *IEEE Trans. Information Theory*, vol. 51, no. 12, pp. 4134-4151, Dec. 2005.
- J24 A. M. Tulino, A. Lozano, and S. Verdú "Impact of Antenna Correlation on the Capacity of Multiantenna Channels," *IEEE Trans. Information Theory*, vol. 51, no. 7, pp. 2491-2509, July 2005.
- J23 A. M. Tulino, L. Li and S. Verdú "Spectral Efficiency of Multicarrier CDMA," *IEEE Trans. Information Theory*, vol. 51, no. 2, pp. 479-505, Feb. 2005.
- J22 A. M. Tulino and S. Verdú, "Random Matrices and Wireless Communications," *Foundations and Trends in Communications and Information Theory*, vol. 1, no. 1, pp.1-182, June 2004.
- J21 L. Li, A. M. Tulino, and S. Verdú "Design of Reduced-rank MMSE Multiuser Detectors using Random Matrix Methods," *EEE Trans. Information Theory*, vol. 50, no. 6, pp. 986-1008, June 2004.
- J20 A. Lozano, A. M. Tulino, and S. Verdú "Multiantenna Capacity in the Low-Power Regime," *IEEE Trans. Information Theory*, vol. 49, no. 10, pp. 2527-2544, Oct. 2003.
- J19 A. Lozano, and A. M. Tulino, "Capacity of Multiple-Transmit and Multiple-Receive Antenna Architectures", *IEEE Trans. Information Theory*, vol. 48, no. 12, pp. 3117-3128, Dec. 2002.
- J18 E. Biglieri, G. Taricco, and A. Tulino, "Decoding space-time codes with BLAST architectures", *IEEE Trans. Signal Processing*, vol. 50, no. 9, pp. 2547-2552, Sep. 2002.
- J17 E. Biglieri, G. Taricco, and A. Tulino, "Performance of space-time codes for a large number of antennas," *IEEE Trans. Information Theory*, vol. 48, no. 7, pp. 1794-1803 July 2002.

- J16 L. Li, A. M. Tulino, and S. Verdú, "Asymptotic Eigenvalue Moments for Linear Multiuser Detection", *Communication in Information and Systems, (invited paper)* vol 1, no. 3, pp. 273-304, Sep. 2001.
- J15 E. Biglieri, and A. M. Tulino, "Designing space-time codes for a large number of receiving antennas", *Electronics Letters*, vol. 37, no. 17, pp. 1073-1074, Aug. 2001.
- J14 A. M. Tulino, and S. Verdú, "Asymptotic analysis of improved linear receivers for BPSK-CDMA subject to fading", *Journal on Selected Areas in Communications, Special Issue on Signal Processing for Wireless Communications*, vol. 19, pp. 1544 -1555, Aug. 2001.
- J13 S. Buzzi, M. Lops, and A. M. Tulino, "A generalized minimum-mean-output-energy strategy for CDMA Systems with improper MAI," *IEEE Trans. Information Theory*, vol. 48, no. 3, pp. 761-767, Mar. 2002.
- J12 S. Buzzi, M. Lops, and A. M. Tulino, "Adaptive Detection and Channel Estimation for Dual-Rate DS/CDMA Networks in Frequency-Selective Fading," *Wireless Personal Communications*, Kluwer Academic Press, vol. 16, no. 3, pp. 259-285, Mar. 2001.
- J11 S. Buzzi, M. Lops, and A. M. Tulino, "Blind Adaptive Multiuser Detection for Asynchronous Dual-Rate DS/CDMA Systems," *Journal on Selected Areas in Communications*, vol. 19, no 2, pp. 233-244, Feb. 2001.
- J10 S. Buzzi, M. Lops, and A. M. Tulino, "Partially Blind Adaptive MMSE Interference Rejection in Asynchronous DS/CDMA Networks over Frequency-Selective Fading channels," *IEEE Trans. on Communications*, vol. 48, no. 1, pp. 94-108, Jan. 2001.
- J9 S. Buzzi, M. Lops, and A. M. Tulino, "A new family of MMSE multiuser receivers for interference suppression in DS/CDMA Systems Employing BPSK Modulation," *IEEE Transactions on Communications*, vol. 48, no. 1, pp. 154-167, Jan. 2001.
- J8 M. Lops and A. M. Tulino, "Simultaneous suppression of multiaccess and narrowband interference in asynchronous CDMA networks," *IEEE Trans. on Vehicular Technology*, vol. 49, no. 5, pp. 1705-1718, Sep. 2000.
- J7 A. M. Tulino, E. Biglieri, and S. Glisic "Iterative interference suppression and decoding," *IEICE Trans. on Communications, (invited paper)*, vol. E83-B, no. 8, pp. 1591-1601, Aug. 2000
- J6 S. Buzzi, M. Lops, and A. M. Tulino, "MMSE RAKE reception for asynchronous DS/CDMA overlay systems and frequency-selective fading channels," *Wireless Personal Communications*, Kluwer Academic Press, vol. 13, no. 3, pp. 295-318, June 2000.
- J5 S. Buzzi, M. Lops, and A. M. Tulino, "Time-varying NBI rejection in asynchronous multiuser DS/CDMA systems over frequency-selective fading channels," *IEEE Trans. on Communications*, vol. 47, pp. 1523-1536, Oct. 1999.
- J4 M. Lops and A. M. Tulino, "Automatic suppression of narrowband interference in direct sequence spread spectrum systems," *IEEE Trans. on Communications*, vol. 47, no. 8, pp. 1133-1136, Aug. 1999.
- J3 G. Gelli, L. Paura, and A. M. Tulino, "Cyclostationary-based filtering for narrow-band interference suppression in direct-sequence spread spectrum systems," *Journal on Selected Areas in Communications, Special Issue on Signal Processing for Wireless Communications*, vol. 16, no. 9, pp.1747-1755, Dec. 1998.

- J2 M. Lops, G. Ricci, and A. M. Tulino, "Narrowband Interference Suppression in Multiuser CDMA Systems," *IEEE Trans. on Communications*, vol.46, no.9, pp.1163-1175, Sep. 1998.
- J1 E. Conte, M Lops, and A. M. Tulino, "Hybrid procedure for CFAR in non-Gaussian clutter," *IEE Proceedings (Radar, Sonar and Navigation)*, vol. 144, no. 6, pp. 361-369, Dec. 1997.

CONFERENCE PAPERS

- C79 A. Aubry, A. M. Tulino, and Sivarama Venkatesan, "Allerton Receiver Cooperation in Gaussian Interference Networks with Imperfect Channel State Information" *Forty-eight Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, Oct. 1-2, 2010.
- C78 G. Alfano, A. Demaio, A. M. Tulino, "Information-theoretic performance analysis of LMS MIMO communications", IEEE Information Theory Workshop, Dublin, Ireland, August 30-Sep. 3, 2010.
- C77 A. Aubry, A. M. Tulino, and Sivarama Venkatesan, "Multiple-Access Channel Capacity Region with Incomplete Channel State Information", *2010 IEEE International Symposium on Information Theory (ISIT2009)*, Austin, TX, USA, June 13-18, 2010.
- C76 P. Memmolo, M. Lops, A. M. Tulino, R. Valenzuela, "Up-Link Multi-User MIMO Capacity in Low-Power Regime", *2010 IEEE International Symposium on Information Theory (ISIT2009)*, Austin, TX, USA, June 13-18, 2010.
- C75 H. Huh, A. M. Tulino, G. Caire, "Network MIMO Large-System Analysis and the Impact of CSIT Estimation", *on Information Sciences and Systems*, Princeton, NJ, Mar. 15-17, 2010.
- C74 A. M. Tulino, G. Caire, S. Shamai, S. Verdú, "Capacity of frequency-selective and time-selective fading channel," *Information Theory and Applications*, San Diego, CA, USA, Jan 31-Feb 4, 2010.
- C73 A. Tulino, G. Caire, S. Shamai, S. Verdú, "The Capacity of the Frequency/Time-Selective Fading Channel," *2010 IEEE Information Theory Workshop*. Cairo, Egypt, Jan. 6-8, 2010.
- C72 A. Tulino, G. Caire, S. Shamai, S. Verdú, "The Capacity of the Frequency/Time-Selective Fading Channel," *2010 IEEE Information Theory Workshop*. Cairo, Egypt, Jan. 6-8, 2010.
- C71 A. Aubry, M. Lops, A. M. Tulino, and L. Venturino, "On MIMO waveform design for non-Gaussian target scattering," *RADAR 2009*, Bordeaux, France, October 12, 2009.
- C70 A. Aubry, L. Lops, A. M. Tulino, and L. Venturino, "Statistical MIMO Radar under non-Gaussian target scattering", *ITW 2009*, Taormina, Sicily, October 11, 2009.
- C69 M. Paturzo, P. Memmolo, A. Tulino, A. Finizio, L. Miccio and P. Ferraro, "Multiplexing and de-multiplexing of digital holograms recorded in microscopic configuration", *3rd EOS Topical Meeting on Optical Microsystem*, 27-30 settembre 2009, Capri, Italy.
- C68 M. Paturzo, P. Memmolo, A. Tulino, A. Finizio, L. Miccio and P. Ferraro, "Numerical multiplexing and de-multiplexing techniques for efficient storage and transmission of digital holographic information," *Fringe 2009 The 6th International Workshop on Advanced Optical Metrology*, 14-17 September 2009, Germany.

- C67 A. Aubry, M. Lops, A. M. Tulino and L. Venturino, "On MIMO detection under non-Gaussian target scattering: The power-limited case.", *2009 IEEE International Symposium on Information Theory (ISIT2009)*, Seoul, Korea, June 28, 2009.
- C66 M. Paturzo, P. Memmolo, A. Tulino, A. Finizio, L. Miccio, P. Ferraro, "Multiplexing and demultiplexing of digital holograms recorded in microscopic configuration," *SPIE Europe Optical Metrology*, 15-18 June 2009, Munich, Germany.
- C65 M.R. McKay, I. B. Collings, and A. M. Tulino, "Exploiting Connections Between MIMO MMSE Achievable Rate and MIMO Mutual Information", *2009 IEEE International Conference on Communications (ICC 2009)*, pp. 1-5, Dresden, Germany, June 14-18, 2009.
- C64 G. Alfano, G.; C. F. Chiasserini, A. Nardio, and A. M. Tulino "Asymptotics of Multi-Fold Vandermonde Matrices with Applications to Communications and Radar Problems", *2009 IEEE International Conference on Communications (ICC 2009)*, pp. 1-5, Dresden, Germany, June 14-18, 2009.
- C63 G. Alfano, M. Guillaud, A. Tulino, High and low-SNR regimes for stochastic networks, *ISITA '08*, Auckland, NZ, December 7-10, 2008.
- C62 G. Alfano, A. Aubry, H. Huang, A. Tulino, "Analysis of Cooperative MIMO Networks with Incomplete Channel State Information," *NWMIMO Workshop, PIMRC 2008*, Cannes, France, September 15-18, 2008.
- C61 G. Alfano, M. Guillaud, A. Tulino, "Scaling Laws for Large Ad-hoc Wireless Networks with Wishart-Poisson Fading," *International Symposium on Spread Spectrum Techniques and Applications (ISSSTA)*, Bologna, Italy, August 25-29, 2008.
- C60 A. Tulino, S. Verdú, G. Caire and S. Shamai (Shitz), "Intersymbol Interference with Flat Fading: Channel Capacity," *2007 IEEE International Symposium on Information Theory (ISIT2007)*, July 6-11, 2008, Toronto, Canada.
- C59 G. Alfano, M. Guillaud, A. Tulino, "The Role of Euclidean Random Matrices in Performance Analysis of Communications and Sensor Networks," *Stochastic Networks Conference (SNC)*, Paris, France, June 23-28, 2008.
- C58 A. Tulino, S. Verdú, G. Caire and S. Shamai (Shitz), "The Gaussian Erasure Channel," *2007 IEEE International Symposium on Information Theory (ISIT2007)*, June 24-29, 2007, Nice, France.
- C57 A. Lozano, A. Tulino and S. Verdú, "Optimum Ergodic Power Allocation for Multiuser OFDM with Arbitrary Signal Constellations", *2006 IEEE Global Communications Conference*, San Francisco, CA, Nov. 27- Dec. 1, 2006.
- C56 A. Lozano, A. Tulino and S. Verdú, "Multiuser Mercury/waterfilling for Downlink OFDM with Arbitrary Signal Constellations", *9th International Symposium on Spread Spectrum Techniques and Applications*, Manaus, Amazon, Brazil, Aug. 28-31, 2006. (*best paper award*).
- C55 J. W. Silverstein and A. Tulino, "Theory of Large Dimensional Random Matrices for Engineers", *9th International Symposium on Spread Spectrum Techniques and Applications*, Manaus, Amazon, Brazil, Aug. 28-31, 2006. (*invited paper*).
- C54 G. Alfano, A. Lozano, A. Tulino and S. Verdú, "Eigenvalue Statistics of Finite-Dimensional Random Matrices for MIMO Wireless Communications", *2006 IEEE International Conference on Communications (ICC 2006)*, Istanbul, Turkey, June 11-15, 2006.

- C53 G. Alfano, A. Lozano, A. Tulino and S. Verdú, "Random Matrix Transforms and Applications Via Nonasymptotic Eigenanalysis," *2006 International Zurich Seminar*, (invited paper), Feb. 22-24, 2006.
- C52 A. Lozano, A. Tulino and S. Verdú, "Mercury/Waterfilling for Fixed Wireless OFDM Systems," *IEEE Radio & Wireless Symposium (RWS)* (invited paper), San Diego, Ca. Jan.. 17-19, 2006.
- C51 A. Lozano, A. Tulino and S. Verdú, "Mercury/Waterfilling: Optimum Power Allocation with Arbitrary Input Constellations," *2005 IEEE Int. Symposium on Information Theory*, Adelaide, Australia, Sep. 4-9, 2005.
- C50 A. Tulino and S. Verdú, "An Application of Random Matrix Theory: Asymptotic Capacity of Ergodic and Non-ergodic Multiantenna Channels," *Joint meeting of the Chinese Society of Probability and Statistics (CSPS) and the Institute of Mathematical Statistics (IMS)*, (invited paper), Beijing on July 9-12, 2005.
- C49 A. Tulino, A. Lozano, and S. Verdú, "High-SNR Power Offset in Multi-Antenna Ricean Channels," *2005 IEEE Int. Conf. Communications*, Seoul, South Korea, May 16-20, 2005
- C48 A. Tulino and S. Verdú, "Asymptotic Outage Capacity of Multiantenna Channels," *2005 IEEE Int. Conf. Acoustics, Speech and Signal Processing*, (invited paper), Philadelphia, Pa, March 18-23, 2005.
- C47 G. Alfano, A. Lozano, A. Tulino and S. Verdú, "Mutual Information and Eigenvalue Distribution of MIMO Ricean Channels," *2004 Int. Symposium on Information Theory and its Applications*, Parma, Italy, Oct. 10-13, 2004.
- C46 A. Tulino, A. Lozano, and S. Verdú, "Power Allocation in Multi-Antenna Communication with Statistical Channel Information at the Transmitter," *2004 IEEE Int. Symposium on Personal, Indoor and Mobile Radio Communications*, Barcelona, Spain, Sep. 5-8, 2004.
- C45 R. Muller and A. Tulino, "Minimum Bit Error Probability of Large Randomly Spread MC-CDMA Systems in Multipath Rayleigh Fading," *2004 IEEE Int. Symposium on Spread Spectrum Techniques and Applications*, Sydney, Australia, Aug. 30-Sep. 2, 2004.
- C44 A. Tulino, A. Lozano, and S. Verdú, "MIMO Capacity with Channel State Information at the Transmitter," *2004 IEEE Int. Symposium on Spread Spectrum Techniques and Applications*, Sydney, Australia, Aug. 30-Sep. 2, 2004.
- C43 G. Alfano, A. Lozano, A. Tulino and S. Verdú, "Capacity of MIMO channels with one-sided correlation," *2004 IEEE International Symposium on Spread Spectrum Techniques and Applications*, Sydney, Australia, Aug. 30-Sep. 2, 2004.
- C42 A. Tulino and S. Verdú, "The Shannon Transform in Random Matrix Theory," *Sixth Bernoulli Society/IMS Congress*, (invited paper), Barcelona, Spain, July 26-30, 2004.
- C41 A. Lozano, A. Tulino and S. Verdú, "High-SNR Power Offset in Multi-Antenna Communication," *2004 IEEE Int. Symposium on Information Theory*, Chicago, IL, June 27-July 2, 2004.
- C40 L. Li, A. Tulino and S. Verdú "Spectral Efficiency of MC-CDMA: Linear and Non-Linear Receivers" *Forty-first Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, Oct. 1-3, 2003.

- C39 A. Lozano, A. Tulino and S. Verdú "Capacity-Achieving Input Covariance for Correlated Multi-Antenna Channels" *Forty-first Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, Oct. 1-3, 2003.
- C38 A. Lozano, A. M Tulino, and S. Verdú, "Multi-antenna capacity in interference-limited low-power conditions", *2003 IEEE Int. Symposium on Information Theory*, Yokohama, June 29 - July 4, 2003.
- C37 L. Li, A. M. Tulino, and S. Verdú, "Design of MMSE multiuser detectors using random matrix methods", *2003 IEEE Int. Conference in Communications*, Alaska, May 11-15, 2003.
- C36 A. M. Tulino, A. Lozano, and S. Verdú, "Capacity of antenna arrays with space, polarization and pattern diversity", *2003 IEEE Information Theory Workshop*, Paris, France, Mar. 30- Apr. 4, 2003.
- C35 A. Lozano, A. M Tulino, and S. Verdú, "Correlation number: a new design criterion in multi-antenna communication", *2003 IEEE Vehicular Technology Conference*, Korea, Apr. 2003.
- C34 E. Biglieri, G. Taricco and A. M. Tulino, "Asymptotic performance analysis of linear interfaces for space-time codes over MIMO fading channels", *2002 Joint Workshop on Communications and Coding, (invited paper)*, Barolo, Italy, Nov. 3-6, 2002.
- C33 A. M. Tulino, S. Verdú, and A. Lozano, "Multi-antenna capacity in the low-power regime", *DIMACS Workshop on Signal Processing for Wireless Transmission, (invited paper)*, Rutgers University, Piscataway, NJ, Oct. 7-9, 2002.
- C32 A. Lozano, A. M Tulino, and S. Verdú, "Capacity of multi-antenna architectures in the low-power regime", *2002 IEEE Information Theory Workshop*, Bangalore, India, Oct. 20-25, 2002.
- C31 E. Biglieri, G. Taricco, and A. M. Tulino, "How far away is infinity? Using asymptotic analyses in multiple-antenna systems", *2002 IEEE Int. Symposium on Spread Spectrum Techniques & Applications*, Prague, Czech Republic, Sep. 2-5, 2002.
- C30 E. Biglieri, G. Taricco, and A. M. Tulino, "Decoding space-time codes with BLAST architectures", *2002 IEEE Int. Symposium on Spread Spectrum Techniques & Applications*, Prague, Czech Republic, Sep. 2-5, 2002.
- C29 E. Biglieri, G. Taricco, and A. M. Tulino, "Decoding space-time codes with BLAST architectures", *2002 IEEE Int. Symposium on Information Theory*, Lausanne, Switzerland, July 2002.
- C28 E. Biglieri, G. Taricco, and A. M. Tulino, "Linear receivers for multiple-antenna communication channels: an asymptotic analysis", *2002 IEEE Int. Conference on Communication*, New York, NY, June 2002.
- C27 E. Biglieri, G. Taricco, and A. M. Tulino, "Performance of space-time codes with linear receiver interfaces", *Conference on Information Sciences and Systems*, Princeton, NJ, Mar. 2002.
- C26 L. Li, A. M. Tulino, and S. Verdú, "Asymptotic Eigenvalue Moments for Linear Multiuser Detection", *35th Asilomar Conference on Signals, Systems, and Computers*, Pacific Grove, Ca, Nov. 4-7, 2001.

- C25 G. Caire, A. M. Tulino, and E. Biglieri, "Iterative multiuser joint detection and parameter estimation: A factor-graph approach", *2001 IEEE Information Theory Workshop (ITW'01)*, Cairns, Australia, Sep. 2-7, 2001.
- C24 E. Biglieri, G. Taricco, and A. Tulino, "Codes and Architectures for multiple antenna transmission systems," *7th International Workshop on Digital Signal Processing Techniques for Space Communications*, Lisbon, Portugal, Oct. 1-3, 2001.
- C23 E. Biglieri, G. Taricco, and A. Tulino, "Asymptotic Performance of Linear Receiver Interfaces for Space-Time Codes," *2001 Int. Symposium on Wireless Personal Multimedia Communications (best paper award)*, Aalborg, Denmark, Sep. 9-12, 2001.
- C22 E. Biglieri, G. Taricco, and A. Tulino, "Performance of space-time codes for a large number of antennas," *2001 Int. Symposium on Telecommunication*, Tehran, Iran, Sep. 1-3, 2001.
- C21 E. Biglieri, G. Taricco, and A. Tulino, "Performance of space-time codes with linear and non-linear receiver interfaces in asymptotic multiple-antenna systems," *8th International Conference on Advances in Communications and Control*, Crete, Greece, June 25-29, 2001.
- C20 E. Biglieri, A. M. Tulino, "Designing Space-Time Codes for Large Number of Receiving Antennas," *Conference on Information Sciences and Systems*, Baltimore, Md., Mar. 2001.
- C19 A. M. Tulino and S. Verdú, "Improved Linear Receivers for BPSK-CDMA Subject to Fading," *38th Annual Allerton Conference on Communication, Control and Computing, (invited paper)*, Monticello, IL, Oct. 4-6, 2000.
- C18 A. M. Tulino and E. Biglieri, "Iterative interference suppression and decoding in DS/FH spread-spectrum systems," *2000 International Symposium on Information Theory and Its Applications (ISITA2000)*, Honolulu, Hawaii, Nov. 5-8, 2000.
- C17 M. Lops and A. M. Tulino, "Linear and linear-conjugate/linear (LC/L) receivers for CDMA systems in fading channels," *2000 IEEE Sixth International Symposium on Spread Spectrum Techniques & Applications*, Parsippany, NJ, Sep. 6-8, 2000.
- C16 S. Buzzi, M. Lops, and A. M. Tulino, "Data-like interference suppression in multiuser CDMA systems: A new family of MMSE detectors," *Conference on Information Sciences and Systems*, Princeton, NJ, Mar. 15-17, 2000.
- C15 S. Buzzi, M. Lops, and A. M. Tulino, "A new class of multiuser CDMA receivers based on the minimum mean-output-energy strategy," *2000 IEEE Int. Symposium on Information Theory*, Sorrento, Italy, June 25-30, 2000.
- C14 S. Buzzi, M. Lops, and A. M. Tulino, "Adaptive MMSE detection for asynchronous dual-rate CDMA systems: Time-varying versus time-invariant receivers," *1999 IEEE Global Communications Conference*, Rio de Janeiro, Brazil, Dec. 5-9, 1999.
- C13 S. Buzzi, M. Lops, and A. M. Tulino, "Blind cyclic interference cancellation for overlay DS/CDMA systems over frequency-selective fading channels," *1999 IEEE 10th International Symposium on Personal Indoor and Mobile Radio Communications*, Osaka, Japan, Sep. 12-15, 1999.
- C12 S. Buzzi, M. Lops, and A. M. Tulino, "MMSE narrowband and multiaccess interference rejection in DS/CDMA asynchronous multipath fading channels," *1999 IEEE 10th*

- International Symposium on Personal Indoor and Mobile Radio Communications*, Osaka, Japan, Sep. 12-15, 1999.
- C11 S. Buzzi, M. Lops, and A. M. Tulino, "Linear-conjugate/Linear filtering for interference rejection in multi-rate DS/CDMA systems," *1999 IEEE Wireless Communications and Networking Conference*, New Orleans, La, Sep. 21-24, 1999.
- C10 S. Buzzi, M. Lops, G. Ricci, and A. M. Tulino, "Blind group detectors for multirate/multicode CDMA systems over frequency-selective fading channels," *1999 Finnish Signal Processing Symposium*, Oulu, Finland, May 29-31, 1999.
- C9 S. Buzzi, M. Lops, G. Ricci, and A. M. Tulino, "Blind adaptive interference suppression for dual-rate CDMA: Time-varying versus time-invariant receivers," *1999 Finnish Signal Processing Symposium*, Oulu, Finland, May 29-31, 1999.
- C8 S. Buzzi, M. Lops, G. Ricci, and A. M. Tulino, "A family of improved baseband MMSE detectors for interference suppression in multiuser CDMA systems," *1999 Finnish Signal Processing Symposium*, Oulu, Finland, May 29-31, 1999.
- C7 S. Buzzi, M. Lops, and A. M. Tulino, "MMSE multiuser detection in multipath fading channels," *1999 IEEE International Conference on Acoustics, Speech, and Signal Processing*, Phoenix, Az, Mar. 1999.
- C6 S. Buzzi, M. Lops, and A. M. Tulino, "Time varying MMSE interference suppression on asynchronous DS/CDMA systems over multipath fading channels," *1998 IEEE 9th International Symposium on Personal Indoor and Mobile Radio Communications*, Boston, Ma, Sep. 8-11, 1998.
- C5 S. Buzzi, M. Lops, and A. M. Tulino, "MMSE multi-user detection for asynchronous dual rate direct sequence CDMA communications," *1998 IEEE 9th International Symposium on Personal Indoor and Mobile Radio Communications*, Boston, Ma, Sep. 8-11, 1998.
- C4 S. Buzzi, M. Lops, and A. M. Tulino, "A time-varying projection receiver for asynchronous DS/CDMA systems with narrowband interference over multipath fading channels," *1998 IEEE Fifth International Symposium on Spread Spectrum Techniques & Applications*, Sun City, South Africa, Sep. 2-4, 1998.
- C3 M. Lops, and A. M. Tulino, "Symbol-by-symbol projection receiver for interference rejection in asynchronous CDMA networks," *1998 IEEE International Symposium on Information Theory*, Cambridge, Ma, Aug. 16-21, 1998.
- C2 M. Lops, G. Ricci, and A. M. Tulino, "A new multiuser detector employing frequency-domain excision," *1996 IEEE 4th International Symposium on Spread Spectrum Systems Techniques and Applications*, Mainz, Germany, Sep. 10-13, 1996.
- C1 M. Lops, G. Ricci, and A. M. Tulino, "Robust multiuser detection for synchronous CDMA systems," *Conference on Information Sciences and Systems*, Princeton, NJ, Mar. 15-17, 1996.

THESES

- D1 A. M. Tulino, "Rivelazione robusta di onde gravitazionali provenienti da Coalescenti Binarie", (Robust detection of gravity waves from coalescent binaries), Graduation Thesis, July 28, 1995, Napoli, Italy.

D2 A. M. Tulino, “Soppressione dell’Interferenza nei Sistemi CDMA”, (Interference suppression in CDMA systems), PhD Dissertation, Seconda Università degli Studi di Napoli, Jan. 25, 1999, Napoli, Italy.

REPORTS

- R1 A. M. Tulino, “Turbo codes in FH-DS and suppression of narrow-band interference,” Technical report, Center for Wireless Communications, Oulu, 1999.
- R2 A. Lozano, A. M. Tulino, S. Verdú, “Multi-antenna capacity in the low-power regime,” *ITD-02-050568M Lucent Technologies Proprietary*, pp. 1-53, 2002.
- R3 A. Lozano, A. Tulino, S. Verdú, “Impact of Correlation on the Capacity of Multi-Antenna Channels”, *ITD-03-44786F, Lucent Technologies Proprietary*, pp. 1-39, 2003.
- R4 A. Lozano, A. Tulino, S. Verdú, “Mutual Information and Eigenvalue Distribution of MIMO Ricean Channels”, *ITD-04-45550L, Lucent Technologies Proprietary*, pp.1-6, 2004.
- R5 A. Lozano, A. Tulino, S. Verdú, “MIMO Capacity with Channel State Information at the Transmitter”, *ITD-04-45549K Lucent Technologies Proprietary*, pp.1-5, 2004.
- R6 A. Lozano, A. Tulino, S. Verdú, “High-SNR Power Offset in Multi-Antenna Communication”, *ITD-04-45548J, Lucent Technologies Proprietary*, pp.1-36, 2004.
- R7 A. Lozano, A. Tulino, S. Verdú, “Capacity of MIMO Channels with One-sided Correlation” *ITD-04-45547H, Lucent Technologies Proprietary*, 2004, pp.1-5.
- R8 A. Lozano, A. Tulino, S. Verdú, “Capacity-Achieving Input Covariance for Single-user Multi-Antenna”, *ITD-04-45193Y, Lucent Technologies Proprietary*, pp. 1-26, 2004.
- R9 A. Lozano, A. Tulino and S. Verdú, “Optimum Power Allocation for Parallel Gaussian Channels with Arbitrary Input Distributions”, *ITD-05-46167G Lucent Technologies Proprietary*, pp.1-35, 2005