CURRICULUM VITAE

Name: Nigel Boston

Addresses: Department of Mathematics,
303 Van Vleck Hall,
480 Lincoln Drive,
Madison, WI 53706, USA

Department of Electrical and Computer Engineering,
3619 Engineering Hall,
1415 Engineering Drive,
Madison, WI 53706, USA

Telephone: 608-263-4753 (UW Math), 608-265-3817 (UW ECE),

Email: boston@math.wisc.edu, boston@engr.wisc.edu, boston@cs.wisc.edu

Webpage: http://www.math.wisc.edu/∼boston/
https://directory.engr.wisc.edu/ece/Faculty/Boston_Nigel/
https://wid.wisc.edu/people/nigel-boston/

Date of Birth: 20 July, 1961

Citizenship: United Kingdom and United States

Marital Status: Married, two children

PhD: 1987, Harvard University, advisor Barry Mazur

Postdoc: 1988-90, U.C. Berkeley, advisor Kenneth Ribet

Employment:

2002- , University of Wisconsin-Madison
Professor (50% Math, 50% ECE)

2008-2009, University College, Dublin, Ireland
Stokes Professor of Pure and Applied Algebra

2006-2007, University of South Carolina
Williams-Hedberg-Hedberg Chair

1990-2002, University of Illinois at Urbana-Champaign
Tenure-track Assistant Professor, Associate Professor (1995-2002)

2016, FIM, ETH Zurich
Visiting Scholar

1996, Harvard University
Visiting Scholar

1993, Jan-Jun, Newton Institute, Cambridge University, UK
Rosenbaum Fellow

1988-1990, U.C. Berkeley
Morrey Assistant Professor

1987-1988, I.H.E.S., France

Appointments:

2002- , Departments of Math and ECE, UW-Madison

2002- , CS Department, UW-Madison (affiliate)

2015- , Wisconsin Institutes for Discovery, Optimization Group (affiliate)

2008-2009, Professor, Maths Sciences, UC Dublin (visiting from 2009)
2008-2009 , Claude Shannon Institute, UC Dublin (affiliate from 2009)
2008-2009, Complex and Adaptive Systems Laboratory, UCD
2006-2007, Department of Math, Univ. of South Carolina
2006-2007 , USC Industrial Math Institute
1990-2002, Department of Mathematics, UIUC (adjunct from 2002)
1999-2002 , Coordinated Science Laboratory, UIUC (adjunct from 2002)
1999-2002, Beckman Institute, UIUC
1999-2004 , UIUC ECE Department affiliation

Education:

1983-1987, Harvard University
Ph.D. 1987, A.M. 1984
1979-1983, Cambridge University, England
Certificate of Advanced Study in Mathematics, 1983
B.A. with 1st class honours in mathematics, 1982 (became M.A. 1986)

Awards:

2012- , Inaugural AMS Fellow
2015-2016, Simons Fellow
2015- , Senior Member, IEEE
2008-2009, Stokes Professorship (Science Foundation of Ireland)
2006-2007 , Williams-Hedberg-Hedberg Professorship, USC
2006-2008, UW Vilas Associates Award
1995-1998, UIUC University Scholar
1994-1996, Alfred P. Sloan Foundation Fellow
1995-1996, Helen Corley Petit Professorship
1995, Finalist, Oakley-Kunde Award for Undergraduate Education
Spring 1995, Arnold O. Beckman Research Award
1993-1994, Center for Advanced Study, Urbana (one semester)
1993, Jan-Jun, Rosenbaum Fellowship, Cambridge Univ.
1986-1987, Sloan Doctoral Dissertation Fellowship
1983-1984, Lounsbery and Wang Fellowships, Harvard

Grants:

2017-2019, NSF & DOE AMPS grant, $220,000, PI
2017-2019, UW2020 Math Institute, $145,000, co-PI
2017-2020, NSF TRIPODS Inst. for Data Science, $1,500,000 (PI S.Wright)
2015-2020, NSF RTG in Alg Geom, Appl Alg, and Number Thy, $2,000,000, PI
2015-2016, Simons Fellow, $98,250, PI
2011-2017, DIMACS Special Focus on Cybersecurity, $699,000 (PI R.Wright)
2009-2013, SFI RFP grant, UCD, $166,000 direct (forced to decline), PI
2008-2009, Stokes Professorship start-up, UCD, $75,000, PI
2009-2011, NSA grant, UW, $60,000, PI
2009-2014, NSF RTG grant, UW, $1,300,000, (PI K.Ono)

2008-2009, UW Graduate School Award "A novel invariant for video tracking in camera sensor networks," $64,500, PI, co-PIs C.Dyer (UW CS) and Y.H.Hu (UW ECE)

2006-2007, Williams-Hedberg-Hedberg fund, USC, $25,000, PI

2006-2008, UW Vilas grant, $83,600, PI

2005-2008, NSF TF grant "Message-passing algorithms: from practice to theory and back to practice," $209,500 (UW portion) PI, UIUC ECE PI R.Koetter, co-PI P.Vontobel (Hewlett-Packard)

2004-2008, NSF MSPA-MCS grant "Face recognition using integral invariants and cryptology," $500,000, PI, co-PIs C.Dyer (UW CS) and Y.H.Hu (UW ECE)

2003-2006, NSF DMS grant "Tree representations and probabilistic zeta functions," $64,000, PI

2003-2007, Cluster Enhancement "Optimization of algorithms and applications," $56,000, PI, co-PIs R.Nowak (UW ECE) and S.Wright (UW CS)

2003-2004, Graduate School Fall Competition "Biologically motivated method for human face recognition", $27,000, PI, co-PI Y.H.Hu (UW ECE)

2002- , UW Computational Sciences Cluster start-up $126,000, PI

2000-2003, Motorola Communications Center grant "Security of elliptic curve cryptosystems," $270,000, PI, co-PI R.Blahut (UIUC ECE)

2000-2003, NSF CRCD grant "A cryptography center for research and education," $546,700, PI, co-PIs R.Blahut (UIUC ECE) and S.H.Teng (UIUC CS)

2000-2003, UIUC-CNRS collaboration $100,000 PI, co-PIs I.Duursma (UIUC Math), F.Morain (CNRS), and P.Solé (CNRS)

1999-2003, NSF DMS grant "The unramified Fontaine-Mazur conjecture," $90,000, PI

1999-2001, NSF DMS grant "Special year in number theory," $60,000, PI

1999-2001, CRI grant "Cryptography, coding theory, and arithmetic geometry," $100,000, PI, co-PI R.Blahut (UIUC ECE)

1998-2001, BSF award (US-Israel) "Positively finitely generated groups and zeta functions," co-PI, PI A.Mann (Hebrew University)

1996-1999, NSF DMS grant "Group theory methods in number theory," $60,000, PI

1995-1996, Helen Corley Petit Professorship, $10,000, PI

1994-1996, Alfred P. Sloan Foundation grant, $30,000, PI

1993-1996, NSF DMS grant "Galois representations and applications," $50,000 PI

1990-1993, NSF-DMS grant, "Explicit deformations of Galois representations," $40,000 PI

Patents: US patent number 7646918 for "Summation invariant and its application to 3D face recognition", with W.Y.Lin and Y.H.Hu.

Thesis: *Deformation theory of Galois representations* , Harvard, 1987

Specialization: Algebraic number theory, group theory, arithmetical geometry, computer algebra systems, coding, cryptography, interdisciplinary mathematics

Ph.D. students: Gebhard Boeckle (1995), W3 Professor, Heidelberg, Germany
David Ose (1995), NSA
Walter Dabrowski (1996), actuary
Judy Walker (1996), Aaron Douglas Professor, Univ. of Nebraska

Yihsiang Liow (1997), assoc prof of CS, Columbia College
Boris Iskra (1998), instructor, Oregon State Univ.
Sharon Brueggeman (1999)
Darrin Doud (1999), prof, Brigham Young Univ.
David Perry (1999), NSA
Doug Kuhlman (2000), ARRIS, Libertyville, IL
Mark Bauer (2001), assoc prof, U. Calgary, Canada
Thomas Kuhnt (2002), Hdi Global SE
Mona Musa (2003), lecturer, Santa Clara University
Michael Bush (2004), assoc prof, Washington and Lee Univ.
Bogdan Petrenko (2004), assoc prof, Eastern Illinois Univ.
Bret Benesh (2005), prof, St. John's University
You-Chiang Yi (2005)
Qian Zhang (2005), Microsoft Research
John Jossey (2006), quant, FINCAD
Wei-Yang Lin (2006), prof, CS dept, Cheng Chung Univ, Taiwan
Nadya Markin (2006), postdoc, Nanyang Tech. U., Singapore
Matthew Darnall (2008), director, Element Capital Management
Christopher Holden (2008), assoc prof, Univ. New Mexico
Mehmet Haluk Sengun (2008), lecturer, Univ. of Sheffield, UK
Jay Wierer (2008), assoc prof, Milwaukee School of Engineering
Harris Nover (2009), Google
Meghan DeWitt (2011), asst prof, St. Thomas Aquinas College
Jonathan Blackhurst (2011), NSA
David Conti (2012), researcher, RobArt, Austria
Rachel Davis (2013), lecturer, UW-Madison
Ting-Ting Nan (2015), Google
Kejia Wang (2016), postdoc, Ocean Networks Canada
Zach Charles (2017), postdoc, ECE dept, UW-Madison
Brandon Alberts (2018), postdoc, U. Connecticut Storrs

Former Masters students: Alison Champion, Madhav Chandrasekher, Steve Harding, Sirin Nitinawarat, and Jake Wallace.

Current Ph.D. students: William Cocke, Vefa Goksel, Jing Hao, Ryan Julian, Woojin Kim, Julia Lindberg, and Yuan Liu.

Postdoctoral advisees: Marcin Mazur, Pascal Vontobel, Rafe Jones, Zev Klagsbrun, and Daniel Pimentel-Alarcon.

Initiatives:

Applied Algebra Days
(co-initiator and organizer of 1st, 2nd, and 3rd)

SC Palmetto Number Theory Series
(co-initiator and organizer of 1st)

UW Wireless and Sensor Networks Consortium
(founding director)

UW Face Recognition Group (CS, ECE, Math)
(co-creator and PI)

Computational Sciences Lectures Series, UW
(initiator and organizer 2003-2007)

Co-creator of UCD-Nottingham joint meetings

Midwest Algebraic Number Theory Days
(creator and organizer of 1st , 4th, 10th, and 12th)

Greenwood-Trjitzinsky Prize Competitions for Undergraduates
(creator and chair/organizer of it for 7 years)

Midwest Arithmetical Geometry in Cryptography (MAGC) workshops
(creator and organizer of 1st, 2nd, and 3rd)

Illinois Center for Cryptography and Information Protection
(founding director)

UIUC Thursday number theory lunches
(started and organized for 8 years)

UIUC Information protection seminars
(started and organized for 2 years)

Algebraic number theory international preprint archives
(co-created and managed for 5 years)

Revision of Math 118 (quantitative reasoning) (and for distance learning)
(introduced new approach and led team of TAs)

Conferences (co-)organized:

2017, BIRS Meeting on Symmetries of Surfaces, Maps, and Dessins
2016, ICERM Cybersecurity conference
2016, 3rd Applied Algebra Day
2015, DIMACS Post-quantum Crypto Conference
2014, 2nd Applied Algebra Day
2013, BIRS Meeting on Dynamics over Finite Fields
2013, Number Theory, Group Theory, and Topology Day
2011, 1st Applied Algebra Day
2009, 12th Midwest Algebraic Number Theory Day
2009, 2nd UCD-Nottingham, number theory meeting
2008, Public lectures by Simon Singh
2008, UCD-Nottingham number theory meeting
2007, Codes and Cryptography, Cirencester 2007 (program committee)
2007, AMS special session on applicable algebra, Davidson
2007, Sensor Networks and Beyond workshop
2006, 1st Palmetto Number Theory Seminar
2006, Vancouver Sequences and Codes meeting
2006, Oberwolfach Pro-p Galois Groups meeting
2005, 10th Midwest Algebraic Number Theory Day
2005, Trends in Wireless Communication workshop
2005, Quantum Computation workshop
2004, Optimization of Eigenvalues workshop
2004, Graphical Models workshop
2003, Computational Vision workshop
2001, 3rd MAGC conference
2001, coding theory sessions, Allerton meeting
2000, 2nd MAGC conference
2000, CEPS data security session, CSL

2000, coding theory sessions, Allerton meeting
2000, Fermat's Last Theorem workshop
2000, Millennial Conference on Number Theory
1999, 1st MAGC conference
1999, AMS special session on Galois representations, UIUC
1997, coding theory sessions, Allerton meeting
1997, 4th Midwest Algebraic Number Theory Day
1995, AMS special session on number theory, Chicago
1993, 1st Midwest Algebraic Number Theory Day

Committees:
Cornell Univ. Math Dept review, 2015
DIMACS Special Focus on Cybersecurity, 2011-17
ANTS11 Program Committee, 2013-14
Univ. Zurich Math Inst. review panel, 2011
Program Committee for Cirencester 2007 and 2011
Brigham Young Univ. Math Dept review, 2010
NSF DMS Committee of Visitors, 2010
DFG (Germany) review panels, 2010, 2013, 2016
ANTS9 and ANTS11 Program Committees, 2009-10, 2013-14
Numerous NSF panels, 1993-2017
International Advisory Board, Claude Shannon Institute, Ireland, 2006-08
Search Committee for new IMI Director, 2006-07
Interdisciplinary Faculty Advisory Committee, UW, 2005-08
Physical Sciences Research Committee, UW, 2003-06
Search Committee for new Math Chair, UIUC, 1999
Math Department Executive Committee, 1996-1998
Illinois MAA director-at-large, 1996-99
Search Committee for new Math Chair, UIUC, 1996
NSF posdoctoral fellowships in math sciences, 1993-97, 2008-9

Refereeing:
Annals of Math, Inventiones, IEEE Transactions in Information Theory, IEEE Transactions in Computers, IMRN, Compositio, Journal of Algebra, Journal of Number Theory, Crelle, Math Annalen, Annales de l'Institut Fourier, CU Press, Math Nachrichten, ...

Editing:
Editor (Journal of Group Theory), 2007-
Editor (Involve), 2006-
Co-editor of the Proceedings of the Millennial Conference in Number Theory, UIUC, May 2000 (publ: A.K.Peters)

Courses Taught:
Computer Algebra Systems, Representation Theory, Cryptography, Algebraic Geometry, Arithmetic Geometry in Coding Theory, Cryptography, and Finance, Commutative Algebra, Quantitative Reasoning, Proof of Fermat's Last Theorem, Mathematics for Elementary Teachers, Elliptic Curves, Algebraic Number Theory, Signals and Systems, Group Theory, Class Field Theory, Homological Algebra, Calculus (various levels), Linear Algebra, Abstract Algebra, Elementary Number Theory, Topology, Information Theory, Error-Correcting Codes, ...

Recent Invited Lectures:

Dec 2018	MATC	Math seminar talk

Apr 2018	Boston, MA	AMS session on number theory
May 2017	Edinburgh, UK	Braids conference
Apr 2017	UW-Milwaukee	MAA sectional meeting plenary
Dec 2016	Columbia, SC	PANTS conference plenary
Dec 2016	USC	Math colloquium
Nov 2016	CUNY	Algebra and cryptography seminar
Nov 2016	CUNY	Joint Columbia-CUNY-NYU number theory seminar
Sep 2016	Clemson	RTG lecture series (4 lectures on applied algebra)
Aug 2016	Lincoln, UK	Groups, rings, and automorphisms conference
Jun 2016	Toronto	Kumar Murty's 60th birthday conference (declined)
Jun 2016	Newcastle, UK	Geometry and computation on groups and complexes confere
May 2016	AIM	Arithmetic dynamics workshop
Apr 2016	ETHZ	Number theory seminar
Mar 2016	Kyushu, Japan	Cryptography seminar (declined)
Mar 2016	Kyushu, Japan	Topology and number theory conference
Mar 2016	Zurich	Coding theory seminar
Mar 2016	EPFL	Number theory seminar
Feb 2016	IHP, Paris	Fundamental inequalities and lower bounds conference
Feb 2016	Arizona State U.	Sunmarc conference plenary (declined)
Jan 2016	U Mass Amherst	Five colleges number theory seminar
Dec 2015	Sheffield, UK	Colloquium and number theory seminar
Dec 2015	Newcastle, UK	Algebra seminar
Sep 2015	UC Dublin	Seminar
Mar 2015	MIT	Research Lab of Electronics seminar
Mar 2015	Amherst, MA	Five Colleges number theory seminar
Jan 2015	UC Dublin	Algebra seminar
Jan 2015	Banff, Canada	Mathematics of communications workshop (declined)
Nov 2014	Greensboro, NC	AMS special session (extended talk)
Sep 2014	Eau Claire, WI	AMS special session (extended talk)
Aug 2014	Prague, Czech Rep.	Algebraic statistics
Aug 2014	Oberwolfach	Topology and number theory workshop
Apr 2014	UIUC	Communications group seminar
Apr 2014	EIU	Math colloquium
Sep 2013	MATC	Information theory talk
Apr 2013	Boulder, Colorado	AMS special sessions (2 talks)
Jan 2013	Technion, Israel	Conference in honor of Jack Sonn (declined)
Dec 2012	Purdue Univ.	Colloquium
Dec 2012	Indiana Univ	Algebra seminar
Nov 2012	U Chicago	Group theory seminar
Nov 2012	U Chicago	Scientific and statistical computing seminar
Oct 2012	Monte Verita, Switz.	Trends in Coding Theory meeting
Oct 2012	Allerton, IL	Conference on Coding, Comm, Control (3 talks)
Sep 2012	Oberwolfach	Topology and number theory workshop
Aug 2012	Vienna, Austria	Profinite groups meeting
Jun 2012	Newcastle, UK	Beauville surfaces meeting
Jun 2012	UC Dublin	Algebra seminar
Apr 2012	Arizona State Univ.	Colloquium and seminar
Jan 2012	Boston	AMS Sessions on math comp and on coding theory
Nov 2011	Dagstuhl	Coding theory conference (declined)

Oct 2011	Lincoln, NE	AMS Sessions on coding theory and on number theory
Sep 2011	Costa Rica	Series of lectures in honor of Galois' 200th anniv.
Aug 2011	Banff	BIRS workshop on network information theory
Jul 2011	Dublin, Ireland	Number theory seminar
Jul 2011	Birmingham, UK	Geometric presentations conference
Apr 2011	U. Penn.	Algebra seminar
Apr 2011	Worcester, MA	AMS Special Session on arithmetic topology
Jan 2011	New Orleans	AMS Special Session on computational algebra
Dec 2010	Warwick U	Mathematics colloquium
Dec 2010	Warwick U.	Electrical engineering colloquium
Aug 2010	Oberwolfach	Low-dimensional topology workshop
Jul 2010	Newcastle, UK	7th IEEE IET CSNDSP (keynote speaker)
Jun 2010	U.Chicago	Group theory seminar
Apr 2010	Padova, Italy	Group theory seminar
Mar 2010	Texas A&M	Groups and dynamics seminar
Mar 2010	Austin, TX	Number theory seminar
Mar 2010	Austin, TX	Colloquium
Mar 2010	UIUC	Communications group seminar
Feb 2010	IEM, Essen, Germany	Number theory seminar
Jan 2010	San Francisco	Algebraic methods in signal processing session
Dec 2009	Galway, Ireland	3rd de Brun workshop on comp alg
Oct 2009	Amherst, MA	Five Colleges number theory seminar
Oct 2009	Smith College	McCoy Lecture
Oct 2009	Penn State	Arithmetic and profinite groups AMS session
Oct 2009	Rutgers	Lie theory/quantum math seminar
Aug 2009	Queens U, Belfast	Workshop on algebra, combinatorics, and dynamics
Jun 2009	Dublin	Student summer institute
Jun 2009	Besancon, France	ALGOL conference series of lectures
Jun 2009	Valencia, Spain	Marty Isaacs birthday conference
May 2009	Newcastle, UK	Pure maths colloquium
May 2009	London, UK	Number theory seminar
May 2009	Dagstuhl, Germany	Algorithms and number theory seminar (declined)
May 2009	Tallaght, Ireland	Pure maths colloquium
May 2009	Cork, Ireland	Workshop on Coding and Crypto
Apr 2009	Oxford	Grunewald's birthday conference
Mar 2009	U Maynooth	Colloquium
Feb 2009	Dublin	1st Irish Cryprography Day
Feb 2009	Shannon Institute	2 day module on graph-based codes
Feb 2009	U Warwick	Number theory seminar
Feb 2009	U Warwick	Colloquium
Feb 2009	U Exeter	Number theory seminar
Dec 2008	Columbia, SC	PANTS VIII conference plenary
Dec 2008	Vienna, Austria	ESI profinite groups conference
Nov 2008	UCD, Ireland	Stokes inaugural lecture
Nov 2008	Royal Holloway U	Information security group seminar
Nov 2008	Royal Holloway U	Colloquium
Nov 2008	UCD, Ireland	UCD-Nottingham meeting
Oct 2008	Banff (BIRS)	Self-similarity workshop (declined)
Sep 2008	U Paris 7, France	Analysis on groups seminar

Jun 2008	Oberwolfach	Profinite groups workshop
Apr 2008	U Nebraska	Colloquium
Jan 2008	U Chicago	Group theory seminar
Nov 2007	Montreal, Canada	Labute retirement conference
Oct 2007	Banff (BIRS)	Low-dimensional topology and number theory
Oct 2007	Clemson, SC	22nd Clemson discrete math conference (declined)
Oct 2007	Chicago, IL	AMS coding theory session
Sep 2007	Orono, ME	Maine-Quebec number theory conference (declined)
Sep 2007	Trentino, Italy	Dan Segal's birthday conference
Sep 2007	Dublin, Ireland	Hamilton geometry/topology workshop
Apr 2007	Wake Forest	SERMON plenary
Apr 2007	U. Wisconsin	Pro-p day
Mar 2007	Davidson College	AMS plenary
Mar 2007	Davidson College	AMS session (Galois cohomology)
Feb 2007	Montreal	QC-VT number theory seminar
Feb 2007	McGill Univ	ECE seminar
Feb 2007	U. Indiana	Algebra seminar
Jan 2007	UC San Diego	Number theory seminar
Jan 2007	UCLA	Sensor Networks 2007
Nov 2006	Wake Forest	CS colloquium
Nov 2006	Georgia Tech	Math colloquium
Nov 2006	Fields Institute	Crypto workshop plenary (declined)
Oct 2006	U. Georgia	Number theory seminar
Sep 2006	Clemson	Applicable algebra seminar
Sep 2006	Columbia, SC	IEEE Student Section
Jul 2006	Berlin, Germany	ANTS VII plenary
Jul 2006	UBC, Vancouver	CNTA meeting
May 2006	ETH Zurich	Engineering colloquium
May 2006	Barcelona, Spain	Number theory seminar
May 2006	East High, Madison	FLT talk for children
Apr 2006	U.Penn	Galois theory conference (declined)
Apr 2006	Durham, NH	AMS session (inverse Galois theory)
Apr 2006	USC	Colloquium
Apr 2006	MATC	Face recognition talk
Mar 2006	SFU, Vancouver	Colloquium
Jan 2006	Beckman Institute	Face recognition seminar
Oct 2005	UBC	Seminar and colloquium
Oct 2005	U.Nebraska	AMS session (coding theory)
Jul 2005	Lausanne, Switzerland	Number theory seminar
Jul 2005	Marseilles, France	Journees arithmetiques plenary
Apr 2005	Colorado State	Colloquium
Feb 2005	Princeton	Applied math colloquium
Feb 2005	Princeton	Number theory seminar
Jan 2005	U. Chicago	Group theory seminar
Dec 2004	MATC, Madison	Cryptography talk
Jul 2004	NCTS, Taiwan	Coding theory special lectures
Jun 2004	Essen, Germany	Frey's birthday conference
Jun 2004	Duesseldorf, Germany	Group theory seminar
May 2004	Berlin, Germany	Humboldt Univ. seminar & colloquium

May 2004	London, UK	Algebra colloquium
May 2004	Oxford, UK	Group theory seminar
May 2004	Cambridge, UK	Number theory seminar
Dec 2003	U. Texas	Number theory seminar
Dec 2003	Texas A&M	Groups and dynamics seminar
Oct 2003	Boulder	AMS coding session
May 2003	ETH Zurich	ECE colloquium
May 2003	Oberwolfach	Profinite groups meeting
May 2003	ETH Zurich	Number theory seminar
Mar 2003	Baltimore	JAMI Knots and primes meeting
Jan 2003	Baltimore	AMS session (knots and primes)
Nov 2002	Amherst,MA	Five Colleges number theory seminar
Nov 2002	MIT	ECE colloquium (LIDS)
Nov 2002	U. of Florida	John Thompson's birthday conference
Oct 2002	Chicago	International law conference

NIGEL BOSTON'S PUBLICATIONS

N.Boston, M.Bush, and F.Hajir, "Heuristics for p-class towers of real quadratic fields." Accepted to Journal of the Institute of Mathematics of Jussieu, 2018 (22 pages).

J.Lindberg, A.Zachariah, N.Boston, and B.Lesieutre, "The geometry of real solutions to the power flow equations." Accepted to appear in Allerton Conference, 2018 (8 pages).

Z.Charles and N.Boston, "Exploiting algebraic structure in global optimization and the Belgian chocolate problem." Accepted to Journal of Global Optimization, 2018 (15 pages).

N.Boston and J.Wang, "The 2-class tower of $\mathbf{Q}(\sqrt{-5460})$." Accepted to Geometry, Algebra, Number Theory, and Their Information Technology Applications (Springer Proceedings in Math and Stats) in honor of Kumar Murty, invited paper, 2018 (9 pages).

N.Boston and J.Hao, "Quasi-quadratic residue codes and hyperelliptic curves." Accepted to AMS CONM volume on "Algebraic curves and their applications.", invited paper, 2018 (12 pages).

A.Zachariah, Z.Charles, N.Boston, and B.Lesieutre, "Distributions of the number of solutions to the network power flow equations." Accepted to invited session, ISCAS 2018 (5 pages).

N.Boston and J.Hao, "The weight distribution of quasi-quadratic residue codes." *Advances in Mathematics of Communication,* May 2018, 12(2): 363-385.

N.Boston and M.M.Wood, "Nonabelian Cohen-Lenstra heuristics over function fields." *Compositio Mathematica* 153 (2017), no. 7, 1372–1390.

N.Boston, M.R.Bush, and F.Hajir (with an appendix by J.Blackhurst) "Heuristics for p-class towers of imaginary quadratic fields." *Math. Annalen* , 368, Jun 2017, 633–669.

D.Pimentel-Alarcón, N.Boston, and R.Nowak, "A characterization of deterministic sampling patterns for low-rank matrix completion." *IEEE Journal of Selected Topics in Signal Processing,*vol. 10, no. 4, 623–636, Jun 2016.

J.Hao and N.Boston, "Quasi-quadratic residue codes and their weight distributions." Proceedings of Allerton Conference, 2016.

D.Pimentel-Alarcón, N.Boston, and R.Nowak, "A characterization of deterministic sampling patterns for low-rank matrix completion." Proceedings Allerton Conference, 2015.

N.Boston "A multivariate weight enumerator for tail-biting trellis pseudocodewords." *Journal of Generalized Lie Theory and Applications* , online 2015.

D.Conti and N.Boston "On the algebraic structure of linear tail-biting trellises." *IEEE Trans. Information Theory* , May 2015, 2283–2299

D.Pimentel-Alarcón, N.Boston, and R.Nowak, "Deterministic conditions for subspace identifiability from incomplete sampling, Proceedings IEEE ISIT 2015

V.Goksel, S.Xia, and N.Boston, "A refined conjecture for factoring iterates of quadratic polynomials over finite fields." *Experimental Mathematics* , Vol 24 (3), 304–311, 2015.

N.Barker, N.Boston, N.Peyerimhoff, and A.Vdovina "An infinite family of 2-groups with mixed

Beauville structures." *International Mathematical Research Notices* , 2014. doi: 10.1093/imrn/rnu045 First published online: March 27, 2014 (18 pages).

N.Boston "A survey of Beauville p-groups." Appeared in Proceedings of Conference on Beauville surfaces, Springer Proc. in Math and Stats 123 (4 pages).

N.Barker, N.Boston, N.Peyerimhoff, and A.Vdovina "Regular algebraic surfaces: Ramification, structures and projective planes." Appeared in Proceedings of Conference on Beauville surfaces, Springer Proc. in Math and Stats 123 (18 pages).

N.Boston and T.-T.Nan "A refinement of the four-atom conjecture." Proceedings of NetCod 2013.

N.Boston "Applications of algebra to communications, control, and signal processing." Book, published by Springer, 2012.

N.Boston "On the Belgian Chocolate Problem and output feedback stabilization: efficacy of algebraic methods." Allerton 2012 Proceedings.

D.Conti and N.Boston "The factorization theorem and new algebraic insights into the theory of linear trellises." Allerton 2012 Proceedings.

N.Boston and T.-T.Nan "Large violations of the Ingleton inequality." Allerton 2012 Proceedings.

D.Conti and N.Boston "Factoring linear trellises." IZS 2012 Proceedings.

N.Barker, N.Boston, and B.Fairbairn "A note on Beauville p-groups." *Experiment. Math.* 21, Issue 3 (2012), 298–306.

R.Jones and N.Boston, "Settled polynomials over finite fields." *Proc. Amer. Math.* Soc. 140 (2012), 1849–1863.

N.Barker, N.Boston, N.Peyerimhoff, and A.Vdovina "New examples of Beauville surfaces." *Monatshefte für Mathematik* 166, no 3-4, (2012), 319–327.

N.Boston and J.Ellenberg "Random pro-p groups and random tame Galois groups." Invited Paper for *Groups, Geometry, and Dynamics* 5(2): 265-280 (2011) in honor of Fritz Grunewald.

D.Conti and N.Boston "Matrix representations of trellises and enumerating trellis pseudocodewords. " Allerton 2011 Proceedings.

W.-Y.Lin, Y.-L.Chiu, K.R.Widder, Y.H.Hu, and N.Boston "Robust and accurate curvature estimation using adaptive line integrals." *EURASIP Journal on Advances in Signal Processing* (2010).

R.Arora, C.R.Dyer, Y.H.Hu, and N.Boston "Matching in camera networks using projective joint invariant signatures." ICDSC 2010 Proceedings.

W.-Y.Lin, K.R.Widder, Y.H.Hu, and N.Boston "An integral-based curvature estimation and its application in face recognition." ICME 2010 Proceedings.

N.Boston and G.McGuire "The weight distributions of cyclic codes with two zeros and zeta functions." *Journal of Symbolic Computation.* 45 (7), 723–733 (2010).

N.Boston "Spaces of constant rank matrices over GF(2)." *Electron. J. Linear Algebra* 20 (2010), 1-5.

K.R.Widder, Y.H.Hu, N.Boston, and W.-Y.Lin "Distortion detection for 3D face recognition performance improvement using eigenmouths." ISCAS 2010 Proceedings.

N.Boston "Large transitive groups with many elements having fixed points." Contemporary Mathematics 524, 11–15, AMS volume in honor of Marty Isaacs (2010).

Z.Hong, K.Liu, N.Boston, and A.Sayeed "Algebraic number precoding for space-time block codes." *IEEE Transactions on Information Theory.* **55,** No. 6, 2696–2704, June 2009.

N.Boston and N.Markin "The fewest primes ramified in a G-extension of **Q**" *Annales des Sciences mathématiques du Québec.* 33 no 2, 145–154 (2009).

K.R.Widder, Y.H.Hu, W.-Y.Lin, and N.Boston "Summation invariant multi-region fusion comparison." ISCAS 2009 Proceedings, May 2009.

N.Boston "Random pro-p groups and random Galois groups." Invited paper, *Annales des Sciences mathématiques du Québec.* **32,** no 2. (2009)

B.R.Barmish and N.Boston "Risk and return considerations in The Weakest Link." *American Math Monthly,* 116 (4), 305–315, April 2009.

N.Boston and R.Jones "The image of an arboreal Galois representation." (Invited paper for Serre's 80th birthday). *Pure & Applied Mathematics Quarterly* Vol 5 (1), 213–225 (2009)

N.Boston and M.Darnall "Elliptic curve and hyperelliptic curve cryptography - fundamentals and implementations." Chap 8, 171–190, "Cryptographic Engineering" (ed. Koc)

K.R. Widder, W.-Y. Lin, N. Boston, and Y.H. Hu "Planar-projective summation invariant features for camera networks." Appeared in ICASSP 2008, 753–756.

Q.Zhang and N.Boston "Stylometric watermarking." Appeared in IIHMSP 2008, 477–480.

J.D.Wierer, W.U.Bajwa, N.Boston, and R.D.Nowak "Characterizing decoding robustness under parametric channel uncertainty." Appeared in 45th Annual Allerton Conference on Communication, Control, and Computing 2007.

K.R. Widder, W.-Y. Lin, N. Boston, and Y.H. Hu "From moving frames to summation invariants: procedures, properties and application." Technical Report ECE-07-05, Dept. Elec. Comp. Eng., University of Wisconsin-Madison, Madison, WI, Sept. 2007.

A.Slater, Y.H.Hu, and N.Boston "Multiscale integral invariants for facial landmark detection in 2.5D data." Appeared in MMSP 2007.

W.-Y.Lin, M.-Y.Chen, K.Widder, Y.H.Hu, and N.Boston "Fusion of multiple facial regions for expression-invariant face recognition." Appeared in MMSP 2007.

W.-Y.Lin, K.-C.Wong, N.Boston, and Y.H.Hu "3D face recognition under expression variations using similarity metrics fusion." Appeared in ICME 2007.

N.Boston and R.Jones "Arboreal Galois Representations." (Invited paper.) *Geometriae Dedicata* 124, (2007) 27–35.

J.D.Wierer and N.Boston "A handwritten digit recognition algorithm using two-dimensional hidden Markov models for feature extraction." Appeared

in ICASSP 2007.

N.Boston and H.Nover "Computing pro-p Galois groups." (Invited paper.) Lecture Notes in Computer Science 4076, ANTS VII, 1-10.

K.C. Wong, W. Y. Lin, Y.H. Hu, N. Boston, and X. Zhang, , "Optimal linear combination of facial regions for improving identification performance." *IEEE Transactions SMC Part-B.* 37, (2007), 1138–1148.

J.D.Wierer and N.Boston "Newton polytopes of two-dimensional hidden Markov models." *Experimental Math.* 16 (2007), 227–237

N.Boston "Galois groups of tamely ramified p-extensions. " *Journal de Théorie des Nombres de Bordeaux* 19 (2007), 59–70.

V.Raghavan, A.M.Sayeed, and N.Boston "Near-optimal codebook constructions for limited feedback beamforming in correlated MIMO channels with few antennas" Appeared in ISIT 2006.

W.-Y.Lin, K.-C.Wong, N.Boston, and Y.H.Hu "Fusion of summation invariants in 3D human face recognition" Appeared in CVPR 2006.

N.Boston "Embedding 2-groups in groups generated by involutions." *Journal of Algebra.* 300 (2006), no. 1, 73-76.

W.-Y.Lin, K.-C.Wong, N.Boston, and Y.H.Hu "3D human face recognition using summation invariants" Appeared in ICASSP 2006.

N.Boston and J.Ellenberg "Pro-p groups and towers of rational homology spheres." *Geometry and Topology.* 10 (2006), 331–334.

W.-Y. Lin, K.-C. Wong, Y.-H. Hu, and N. Boston "Face recognition using 3D summation invariant features" Appeared in ICME 2006.

N.Boston "Graph-based codes." Invited paper, in "Recent trends in coding theory and its applications", AMS/IP monograph 41 (2007), 91–122.

N.Boston "Galois p-groups unramified at p - a survey." Invited paper, AMS Contemporary Math series 416 (2006) "Primes and knots", 31–40.

W.-Y.Lin, N.Boston, and Y.H.Hu "Summation invariant features for 3D face recognition." Appeared in Proceedings of MMSP 2005.

S.Nitinawarat and N.Boston "A complete analysis of space-time group codes." Appeared in Proceedings of the 43rd Annual Allerton Conference on Communication, Control, and Computing 2005.

A.Ganesan and N.Boston "Universally decodable matrices." Appeared in Proceedings of the 43rd Annual Allerton Conference on Communication, Control, and Computing 2005.

V.Raganthan, A.Sayeed, and N.Boston "When is limited feedback for transmit beamforming beneficial?" Appeared in Proceedings of ISIT 2005.

N.Boston "Reducing the Fontaine-Mazur conjecture to group theory."

Invited paper, in "Progress in Galois Theory" (Voelklein, Shaska eds.), the proceedings of Thompson's 70th birthday conference, 39-50, 2005.

W.Y.Lin, N.Boston, and Y.H.Hu "Summation invariant and its applications to shape recognition." Appeared in Proceedings of ICASSP 2005.

Q.Zhang and N.Boston "A cryptanalytic method for embedding video watermarks." Appeared in Proceedings of ICASSP 2005.

N.Boston "Pipelined IIR filter architecture using pole-radius minimization." *Journal of VLSI Signal Processing* , 39, 323-331, 2005.

N.Boston and I.M.Isaacs "Class numbers of p-groups of a given order." *Journal of Algebra* 279 (2004), no. 2, 810-819.

N.Boston "Strategies for the Weakest Link." *Amer. Math. Monthly* 110 (2003), no. 4, 330-334.

Q.Zhang and N.Boston "Quantization index modulation using the E_8 lattice." Appeared in Proceedings of the 41st Annual Allerton Conference on Communication, Control, and Computing 2003.

N.Boston "Is biometrics measuring up?" *Journal of Law, Technology, and Policy* 2, (Fall 2002), 421-423.

N.Boston and C.R.Leedham-Green "Explicit computation of Galois p-groups unramified at p." *Journal of Algebra* 256 (2002) no. 2, 402-413.

N.Boston, C.Clancy, Y.Liow, and J.Webster "Genus two hyperelliptic curve coprocessor." Appeared in Proceedings of CHES 2002.

N.Boston "Makhoul's conjecture for p = 2." Appeared in Proceedings of ICASSP 2001.

N.Boston "Bounding minimum distances of cyclic codes using algebraic geometry." Appeared in Proceedings of WCC 2001. Electronic Notes in Discrete Math, Volume 6, April 2001, 385-394.

N.Boston and J.L.Walker "2-groups with few conjugacy classes." *Proc. Edinburgh Math. Soc.* (2) 43 (2000), no. 1, 211-217

N.Boston "The educational use of computer algebra systems at the University of Illinois." (Invited paper) "Handbook of Computer Algebra: Foundations, Applications, Systems" (Grabmeier, Kaltofen, Weispfenning eds.), Springer 2001.

N.Boston "P-adic Galois representations and pro-p groups." Proceedings of the Durham 1997 Pro-p groups meeting. (Invited paper) "New horizons in pro-p groups." (du Sautoy, Segal, Shalev eds.) Birkhaüser 2000.

N.Boston and D.Perry "Maximal 2-extensions with restricted ramification." *Journal of Algebra* 232 (2000), no. 2, 664-672.

N.Boston and D.Ose "Characteristic p Galois representations that are produced by Drinfeld." *Canadian Math. Bull.* 43, no. 3, 282-293 (2000)

S.Basu and N.Boston "Identifiability of polynomial systems." UIUC Technical Report.

N.Boston "Some cases of the Fontaine-Mazur conjecture, II." *Journal of Number Theory* 75, no. 2, 161-169 (1999)

N.Boston "The unramified Fontaine-Mazur conjecture." Procs of the ESF Conference on Number Theory and Arithmetical Geometry, Spain 1997.

N.Boston and C.R.Leedham-Green "Counterexamples to a conjecture of Lemmermeyer." *Arch. Math. (Basel)* 72, no. 3, 177-179 (1999)

N.Boston "The minimum distance of the $[137, 69]$ binary quadratic residue code." *IEEE Transactions in Information Theory* 45, no. 1, 282 (1999)

N.Boston "A use of computers to teach group theory and introduce students to research." *Journal of Symbolic Computation* 23, 453-458 (1997)

N.Boston "Some calculus and open problems in finite group theory." in "Proceedings of the First Jamaican Conference on Group Theory and its Applications" (1997)

N.Boston "A probabilistic generalization of the Riemann zeta function." in "Analytic Number Theory: Proceedings of a Conference in Honor of Heini Halberstam, Volume I" (1996)

N.Boston "A Taylor-made plug for Wiles' proof." *College Mathematics Journal* 26 (2), 100-105 (1995)

N.Boston and A.J.Granville "Review of Marilyn vos Savant's book "The world's most famous math problem" " *American Mathematical Monthly,* 102, 470-473 (1995)

N.Boston "A refinement of the Faltings-Serre method." Séminaire de Théorie des Nombres, Paris, 1992-93

N.Boston and M.L.Greenwood "Quadratics representing primes." *American Mathematical Monthly* 102, 595-599 (1995)

N.Boston, W.Dabrowski, T.Foguel, P.Gies, D.Jackson, J.Leavitt, and D.Ose "The proportion of fixed-point-free elements of a transitive permutation group." *Communications in Algebra* 21 (9), 3259-3275 (1993)

N.Boston and S.V.Ullom "Representations related to CM elliptic curves." *Mathematical Proceedings Cambridge Philosophical Society* 113, 71-85 (1993)

N.Boston "Some cases of the Fontaine-Mazur conjecture." *Journal of Number Theory* 42, 285-291 (1992)

N.Boston "Families of Galois representations - increasing the ramification." *Duke Mathematical Journal* 66, 357-367 (1992)

N.Boston, H.W.Lenstra,Jr. and K.A.Ribet "Quotients of group rings arising from two-dimensional representations." *C. R. Acad. Sci. Paris,* t.312, Série I, p.323-328 (1991)

N.Boston "Explicit deformation of Galois representations." *Inventiones Mathematicae* 103, 181-196 (1991)

N.Boston "Review of the book, "Perfect Groups", by D.Holt and W.Plesken", *Math. Comp.* 57 no. 195, July 1991, 445-446

N.Boston and B.C.Mazur "Explicit universal deformations of Galois representations." *Advanced Studies in Pure Mathematics* 17, 1-21 (1989)

N.Boston "Deformations of Galois representations associated to the cusp form Δ." Séminaire de Théorie des Nombres, Paris, 1987-88

N.Boston Appendix to B.Mazur and A.Wiles, "On p-adic analytic families of Galois representations." *Compositio Mathematica* 59, 231-264 (1986)

N.Boston "A class of soluble groups." *Journal of Algebra* 91, 320-327 (1984)

In Preparation:

N.Boston and T.-T.Nan, "Large violations of the Ingleton inequality and a revised Four-Atom conjecture." Invited paper for issue of Kybernetika in honor of Fero Matus.

N.Boston and M.R.Bush, "Heuristics for 2-class towers of cyclic cubic fields."

J.Lindberg, N.Boston, and B.Lesieutre, "An algebraic approach to improved workspace calculation for optimized redundant robots."

M.R.Julian, D.Papailiopoulos, and N.Boston, "Learning neural networks from a function oracle."