

William J. Martin, 7 Red Barn Road, Holden, MA 01520

H: (508) 829-9727 W: (508) 831-5316 cell: (774) 345-0000 e-mail: martin@wpi.edu

EDUCATION:

Ph.D., Combinatorics & Optimization; 1992, University of Waterloo, Waterloo, Ontario, Canada

M.A., Mathematics (with distinction); 1986, State University of New York at Potsdam

B.A., Computer Science and Mathematics; 1986, State University of New York at Potsdam, Potsdam, NY

PERSONAL:

Date of Birth: 4 July 1962;

U.S. Citizen; Canadian citizen; married; two children.

POSITIONS HELD:

Visiting Scholar, Mathematics, Massachusetts Institute of Technology (July 2006 to June 2007) Research.

Associate Professor, Mathematical Sciences and Computer Science, Mathematical Sciences, Worcester Polytechnic Institute (August 2000 to present) Externally funded research, teaching, service.

Associate Department Head, Mathematical Sciences, Worcester Polytechnic Institute (July 2004 to June 2006) Administrative duties, managing the teaching mission of the department.

Visiting Associate Professor, Center for Applied Cryptographic Research, University of Waterloo (July 1999 to July 2000) Research.

Associate Professor, Mathematics & Statistics, University of Winnipeg (July 1998 to September 2001) Externally funded research; teaching at all undergraduate levels; administrative duties.

Assistant Professor, Mathematics & Statistics, University of Winnipeg (Sept. 1993 to June 1998)

Visiting Assistant Professor, Mathematics & Statistics, University of Vermont (Sept. 1992 to Sept. 1993) Research; teaching at graduate and undergraduate levels.

Visiting Lecturer, Postdoctoral Fellow, Combinatorics & Optimization, University of Waterloo (May to Aug., 1992). Research; teaching.

Summer Research Associate, Government Network Planning Center, AT&T Bell Laboratories, Holmdel, NJ (Summers 1986, 1987, 1988) Programming; some research in graph theory and optimization.

RESEARCH INTERESTS:

Applications of algebra and combinatorics to problems in computer science and mathematics. Structure of association schemes, especially the study of designs and codes within association schemes. Combinatorial methods in cryptography. Also: graph theory; computational complexity; graph algorithms and networks; algebra; topological methods in combinatorics.

PUBLICATIONS: (*refereed, unless otherwise denoted*)

1. W.J. MARTIN AND J.S. WILLIFORD, "There are finitely many Q -polynomial association schemes with given first multiplicity at least three." To appear, *Europ. J. Combin.*
2. C.D. GODSIL, S.A. HOBART AND W.J. MARTIN, "Representations of directed strongly regular graphs," *Europ. J. Combin.* vol. **28** no. 7 (2007), 1980–1993.
3. W.J. MARTIN, M. MUZYCHUK AND J.S. WILLIFORD, "Imprimitive cometric association schemes: constructions and analysis," *J. Algebraic Combin.* vol. **25** no. 4 (2007), 399–415.
4. W.J. MARTIN AND T.I. VISENTIN, "A dual Plotkin bound for (T, M, S) -nets," *IEEE Trans. Inform. Theory*, vol. **53** no. 1 (2007), 411–415..
5. W.J. MARTIN, D.R. STINSON AND B. SUNAR, "A provably secure true random number generator with built-in tolerance to active attacks." *IEEE Trans. Computers*, vol. **56** no. 1 (2007), 109–119.
6. W.J. MARTIN, M. MUZYCHUK AND J.S. WILLIFORD, "Some new constructions of imprimitive cometric association schemes," To appear, proceedings of "Algebraic Combinatorics", an international conference in honour of Eiichi Bannai's 60th birthday, June 26-30, 2006, Sendai, Japan (not refereed).
7. W.J. MARTIN, " (t, m, s) -Nets" (6 pages), a section in the CRC Handbook of Combinatorial Designs (2nd ed.), C.J. Colbourn and J.H. Dinitz, eds., CRC Press (2006) (invited, not refereed).
8. W.J. MARTIN, "Completely regular codes: a viewpoint and some problems." *Proceedings of 2004 Com2MaC Workshop on Distance-Regular Graphs and Finite Geometry*, July 24 - 26, 2004, Pusan, Korea (invited, not refereed).
9. W.J. MARTIN AND B.E. SAGAN, "A new notion of transitivity for sets of permutations." *Journal of the London Mathematical Society*, vol. **73** (2006), 1–13.
10. A.E. BROUWER, C.D. GODSIL, J.H. KOOLEN AND W.J. MARTIN, "Width and dual width of subsets in polynomial association schemes." *J. Combin. Th. Ser. A*, vol. **102** (2003), 255–271.
11. W.J. MARTIN, "A physics-free introduction to quantum error-correcting codes." *Util. Math.* vol. **65** (2004), 133–158.
12. W.J. MARTIN, "Symmetric designs, sets with two intersection numbers and Krein parameters of incidence graphs." *J. Combin. Math. Combin. Comput.* vol. **38** (2001), 185–196.
13. W.J. MARTIN, "Design systems: combinatorial characterizations of Delsarte T -designs via partially ordered sets." pp. 223–239 in: Codes and Association Schemes, ed. A. Barg and S. Litsyn. AMS DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. **56**, 2001.

-
14. W.J. MARTIN, "Minimum distance bounds for s -regular codes." *Des. Codes Cryptogr.* vol. **21** (Special issue dedicated to Dr. Jaap Seidel on the occasion of his 80th birthday, Oisterwijk, 1999.) (2000), 181-187.
 15. W.J. MARTIN, "Linear programming bounds for ordered orthogonal arrays and (T, M, S) -nets." pp368-376, in: *Monte Carlo and quasi-Monte Carlo Methods 1998* (Claremont, CA) (eds. H. Niederreiter and J. Spanier), Springer-Verlag, Berlin, 2000.
 16. W.J. MARTIN AND D.R. STINSON, "Association schemes for ordered orthogonal arrays and (T, M, S) -nets." *Canad. J. Math.* vol. **51** no. 2 (1999), 326-346.
 17. W.J. MARTIN AND D.R. STINSON, "A generalized Rao bound for ordered orthogonal arrays and (t, m, s) -nets." *Canad. Math. Bull.* vol. **42** no. 3 (1999), 359-370.
 18. W.J. MARTIN, "Designs in product association schemes." *Des. Codes Cryptogr.* vol. **16** no. 3 (1999), 271-289.
 19. W.J. MARTIN, "Completely regular designs." *J. Combin. Designs* vol. **6** no. 4 (1998), 261-273.
 20. W.J. MARTIN, "Mixed block designs." *J. Combin. Designs* vol. **6** no. 2 (1998), 151-163.
 21. J.H. DINITZ AND W.J. MARTIN, "The stipulation polynomial of a uniquely list-colorable graph." *Australasian J. Combin.* vol. **11** (1995), 105-115.
 22. W.J. MARTIN AND X.J. ZHU, "Anticodes for the Grassman and bilinear forms graphs." *Designs, Codes and Crypt.* vol. **6** (1995), 73-79.
 23. C.D. GODSIL AND W.J. MARTIN, "Quotients of association schemes." *J. Combin. Th. Ser. A*, vol. **69**, no. 2 (1995), 185-199.
 24. W.J. MARTIN, "Completely regular designs of strength one." *J. Alg. Combin.* vol. **3** (1994), 177-185.

REPORTS: (*non-refereed*)

- W.J. MARTIN, Completely Regular Subsets, Ph.D. dissertation, Department of Combinatorics and Optimization, University of Waterloo, Canada
- W.J. MARTIN, "Completely regular codes in the Odd graphs."
- W.J. MARTIN AND R.R. ZHU, "On the classification of distance-regular graphs by eigenvalue multiplicity." University of Waterloo Research Report CORR 92-06, 1992.
- W.J. MARTIN, "SurvNet: a survivable network design tool. User's guide and programmer's manual" AT&T Bell Laboratories internal memorandum (23 pages), 1987.

HONOURS AND AFFILIATIONS:

- Fellow, Institute for Combinatorics and its Applications
- Member, American Mathematical Society
- Member, Mathematical Association of America
- Member, Society for Industrial and Applied Mathematics

TEACHING EXPERIENCE:

Courses delivered (for example, 3000 level represents a course aimed at 3rd year undergraduates):

1000-2000 level

Calculus
Linear Algebra
Discrete Mathematics
Number Theory
Combinatorics
Applied Algebra
Math of Decision Making

3000 level

Advanced Calculus
Modern Algebra
Intro. Topology
Linear Programming
Mathematical Discovery and Invention

5000 level

Algebra
Graph Theory
Discrete Mathematics I
Hardness vs. Randomness

Individualized Reading Courses

Graph Algorithms
Error-Correcting Codes
Algebraic Geometry
Hyperelliptic Curve Cryptography
Quantum Algorithms

GRANTS:

Awarded:

- National Security Agency (PI): *Problems in association schemes* (Jan. 2007 to Jan. 2009). \$59,000.
- CIMPA (International Centre for Pure and Applied Mathematics, Nice, France): Summer School on SemiDefinite Programming Techniques in Coding Theory, Manila, Philippines
- Slovenian Research Agency (ARRS) (participant): *Open problems in association schemes* 2006–2008. \$19,000.(A. Jurišić, PI)
- National Security Agency (PI): Conference Grant *Discrete Mathematics Day at WPI*, 2005. \$1,500.
- NSF (co-PI): Equipment Grant *Mathematical Sciences Computational Research Environment (SCREMS)*, 2005. \$125,328. (M. Humi, PI)
- National Security Agency (PI): Conference Grant *Discrete Mathematics Day at WPI*, 2003. \$3,000.
- NSF (co-PI): Information Technology Research *Implementing Public-Key Cryptosystems for Secure Information Infrastructure*. \$436,000 (3 years starting 2002). (B. Sunar, PI)
- MITACS, a Canadian Network of Centres of Excellence, (Team member, on a team of twelve researchers): —it Project in Elliptic Curve Cryptography and Algebraic Combinatorics. Cdn \$291,000 per year (S. Vanstone, PI)
- National Science and Engineering Research Council (PI): Individual Grant. Cdn \$48,500 (April 1997 to March 2001)
- National Science and Engineering Research Council (PI): Individual Grant. Cdn \$24,000 (April 1994 to March 1997)

-
- National Science and Engineering Research Council (PI): Equipment Grant. Cdn \$16,000 (April 1996)
 - National Science and Engineering Research Council (co-PI): Equipment Grant. Cdn \$30,000 (April 1994)
 - University of Winnipeg Start-up grant (PI). Cdn \$9,176 (1993-4)

Pending:

- National Science Foundation (co-PI): *CT-ER: Exploring Physical Functions for Lightweight and Robust Cryptography*, \$200,000 (B. Sunar, PI)

RECENT SERVICE ACTIVITIES:

- Chair, Graduate Committee, Mathematical Sciences, Worcester Polytechnic Institute, 2007-2008 academic year.
- Grant proposal reviewer, National Security Agency
- Associate Department Head, Mathematical Sciences, Worcester Polytechnic Institute, July 2004 to June 2006.
- Special session organizer, “Computer Algebra and Combinatorics” ASCM '05, Seoul Korea, December 2005.
- Workshop proposal reviewer, European Science Foundation
- Grant proposal reviewer, Austrian Science Fund.
- Organizing committee chair, Discrete Mathematics Day at WPI (September 2005)
- Book proposal reviewer, Cambridge University Press.
- NSF panel member, Washington
- Organizing committee chair, Discrete Mathematics Day at WPI (May 2003)
- Organizing committee member, Winnipeg Combinatorial Mathematics Conferences (September 1998, September 2000)
- referee for over ten journals in the past four years

RESEARCH STUDENT SUPERVISION:

Postdoctoral Fellow:

- Hajime Tanaka (Ph.D. Kyushu University, Japan), 2007

MSc:

- Ronald Lesniak (project, Industrial Math, 2006)
- Serdar Pehlivanoglu (thesis, CS, 2005) “*Rijndael Circuit-Level Cryptanalysis*”

SELECTED LECTURES:

Upcoming:

- Invited Speaker (60 mins), Ontario Combinatorics Workshop, Toronto, May 23-24, 2008
- Invited Session Organizer, SIAM Conference on Discrete Mathematics, Burlington VT, June 2008 (also speaking)
- Invited plenary lecturer (60 mins), Geometric and Algebraic Combinatorics 4, Oisterwijk, the Netherlands, August 17-22, 2008

Past:

- Algebraic Combinatorics Seminar, University of Waterloo, March 2008
- Undergraduate Lecture, SUNY Potsdam, November 2007
- Combinatorics Seminar, University of Vermont, October 2007
- WPI Cool Math Talk “*Kissing Numbers*”, October 2007
- 21st British Combinatorial Conference, Univ. of Reading, July 2007
- Combinatorics Study Group, Queen Mary University of London, July 6, 2007
- Cryptography Seminar, University of Ljubljana, July 3, 2007
- Bled '07, Bled, Slovenia, June 25, 2007
- Combinatorics seminar, MIT (February and April 2007)
- Invited speaker, Japan-Korea Workshop on Algebra and Combinatorics, Kyushu Univ, Fukuoka, Japan (October 22, 2006)
- Colloquium, College of the Holy Cross (January 2005)
- Combinatorics Seminar, Mt. Holyoke College (November 2004)
- Combinatorics Seminar, University of Delaware (October 2004)
- Invited speaker, 2004 Com2MaC Workshop on Distance-Regular Graphs and Finite Geometry, Busan, Korea (July 24 - 26, 2004).
- Invited speaker, 2004 Com2MaC Conference on Association Schemes, Codes and Designs, Pusan National University, Busan, Korea (July 19 - 23, 2004).
- Invited speaker, Minisymposium on “Geometric and Combinatorial Methods in Coding Theory,” SIAM Conf. Discrete Math., Nashville, TN (June 13-16 2004).
- Colloquium, University of Vermont (November 2003)
- Invited speaker, Workshop on Asymptotic and Computational Aspects of Coding Theory. Institute for Advanced Study, Princeton, NJ (March 24–30, 2001).
- Invited speaker, MSRI Workshop on Emerging Applications of Combinatorial Designs. Berkeley, CA (November 2000).
- Invited speaker, DIMACS Workshop on Codes and Association Schemes. Rutgers University, New Brunswick, NJ (November 1999).
- Invited speaker, IMA Workshop on Coding Theory and Cryptography. Minneapolis, MN (July 1998).