

September 7, 2016

Michael E. O’Sullivan

Professor of Mathematics
Department of Mathematics and Statistics
San Diego State University
San Diego, California, 92182
mosulliv@math.sdsu.edu
<http://www-rohan.sdsu.edu/~mosulliv>

- Education** PH.D. MATHEMATICS: University of California at Berkeley, 1996.
M.S. MATHEMATICS: Portland State University, 1985.
B.A. MATHEMATICS: Reed College, 1981.
- Employment** CHAIR: Department of Mathematics and Statistics, San Diego State University (8/2014 - present).
PROFESSOR: Department of Mathematics and Statistics, San Diego State University (6/2011 - present).
ASSOCIATE PROFESSOR: Department of Mathematics and Statistics, San Diego State University (6/2006 - 6/2011).
ASSISTANT PROFESSOR: Department of Mathematics and Statistics, San Diego State University (8/2000 - 6/2006).
RESEARCHER Center for Communications Research, Institute for Defense Analysis, San Diego, CA, (6-8/2009, 6-8/2011).
VISITING COLLEGE LECTURER: National University of Ireland, Cork, Ireland, (8/1998 - 8/2000).
VISITING RESEARCH ASSISTANT PROFESSOR: Coordinated Science Laboratory, University of Illinois, Urbana-Champaign (6/1998 - 7/2002).
ASSISTANT PROFESSOR OF MATHEMATICS: University of Puerto Rico, Mayaguez (8/1996 - 7/1998).
MATHEMATICIAN: O’Sullivan Consulting Incorporated (6/1989 - 6/1997).
- Grants** PROVOST’S INNOVATION FOR EXCELLENCE AWARD “Improving Student Success and Conceptual Understanding in Calculus,” PI: M. E. O’Sullivan, CoPIs: J. Bowers, R. Carretero, S. Kirshvink, C. Rasmussen, (6/2016-9/2016).
PRESIDENT’S LEADERSHIP FUND “A Discrete Mathematics Problem Library for Online Homework,” PI: M. E. O’Sullivan, CoPI: T. Schmidt, (1/2013-7/2014).
PRESIDENT’S LEADERSHIP FUND “Incorporating Computational Software into Mathematics Courses,” (1/2010 - 9/2012).
NATIONAL SCIENCE FOUNDATION Directorate for Computer and Information Science and Engineering, “Decoding of Algebraic Geometry Codes: Theoretical Analysis, Efficient Algorithms, Practical Implementation,” PI: M. O’Sullivan, (7/2009 - 6/2012) .

NATIONAL SCIENCE FOUNDATION Directorate for Computer and Information Science and Engineering, “Collaborative Research: Improving Low-Density Parity-Check Codes Through Algebraic Analysis of the Sum-Product Algorithm,” PIs: M. O’Sullivan, J. Brevik (CSULB), R. Wolski (UCSB) (2/2007 - 2/2010).

KOREA RESEARCH FOUNDATION, Postdoctoral Foreign Study Grant, PI M. E. O’Sullivan (7/2005 - 6/2006).

SDSU TRAVEL GRANT, “Research Collaboration in Applied Algebra with the National University of Ireland.” (5-6/2004).

NATIONAL SCIENCE FOUNDATION Division of Networking and Communication Research and Infrastructure: “High-Performance Decoding of Algebraic Codes beyond their Packing Radii,” PI R. Blahut (UIUC) (8/2000 - 7/2003). I was an Investigator.

NATIONAL SCIENCE FOUNDATION Division of Networking and Communication Research and Infrastructure grant, “Implementation and Applications of Practical Codes on Curves,” PI R. Blahut (UIUC), Co-PI M. O’Sullivan, (7/1998 - 6/2000).

NATIONAL SCIENCE FOUNDATION Small Business Innovations Research Grant, “Construction of a Decoder for an Algebraic Geometry Code,” PI M. O’Sullivan. Phase I (2-10/1993), Phase II (7/1994 - 9/1996).

DEPARTMENT OF ENERGY Small Business Cooperative Research and Development Grant (9-12/1994).

Book Chapter M. E. O’Sullivan, M. Bras-Amoros: “The Key Equation for One-Point Codes,” Chapter 3, pp. 99-152, of *Advances in Algebraic Geometry Codes*, E. Martinez-Moro, C. Munuera, D. Ruano (eds.), World Scientific, 2008.

Articles in Refereed Journals

K. Bari, M. E. O’Sullivan, “The Hamiltonian problem and t -path traceable graphs,” *Involve*, to appear.

K. Lee, M. Bras-Amorós, M. E. O’Sullivan, “Unique decoding of general AG codes,” *IEEE Transactions on Information Theory*, 60 (2014), no. 4, pp. 2038-2053.

F. Hernando, M.E. O’Sullivan, D. Ruano, “List decoding of repeated codes,” *Applicable Algebra in Engineering, Communications and Computing*, 24 (2013), no. 3-4, pp. 237-253.

F. Hernando, K. Marshall, M. E. O’Sullivan, “The dimension of subcode-subfields of shortened generalized Reed-Solomon codes,” *Designs, Codes, Cryptography*, 69 (2013), pp. 131-142.

K. Lee, M. Bras-Amoros, M. E. O’Sullivan, “Unique Decoding of Plane AG Codes via Interpolation,” *IEEE Transactions on Information Theory*, 58 (2012) no. 6, 3941- 3950.

K. Lee, M. E. O’Sullivan, “Algebraic Soft-Decision Decoding of Hermitian Codes” *IEEE Transaction on Information Theory*, 56 (2010), no 6, 2587-2600.

K. Lee, M. E. O’Sullivan, “List Decoding of Hermitian Codes using Groebner Bases” *Journal of Symbolic Computation*, 40 (2009), no. 12, 1662–1675.

- K. Lee, M. E. O’Sullivan, “Sudan’s List Decoding of Reed-Solomon Codes from a Groebner Basis Perspective” *Journal of Symbolic Computation*, 43 (2008), no. 9, 645–658.
- M. Bras-Amorós, M. E. O’Sullivan, “Redundancies of Correction-Capability-Optimized Reed-Muller Codes” *Discrete Applied Mathematics* 156 (2008), no. 15, 3005–3010.
- M. Bras-Amorós, M. E. O’Sullivan, “Duality for Several Families of Evaluation Codes,” *Advances in the Mathematics of Communications*, 2 (2008), no. 1, 15–33.
- M. Bras-Amorós, M. E. O’Sullivan, “The Order Bound on the Minimum Distance of the One-Point Codes Associated to a Garcia-Stichtenoth Tower of Function Fields” *IEEE Transactions on Information Theory*, 53, (2007), no. 11, 4241–4245.
- M. Bras-Amorós, M. E. O’Sullivan, “On Semigroups Generated by Two Consecutive Integers and Improved Hermitian Codes,” *IEEE Transactions on Information Theory*, 53 (2007), no. 7, 2560–2566.
- E. Byrne, M. Greferath, M. E. O’Sullivan, “The Linear Programming Bound for Codes over Finite Frobenius Rings,” *Designs, Codes and Cryptography*, 42 (2007), no. 3, 289–301. “Errata for: ‘The linear programming bound for codes over finite Frobenius rings’ ” *Designs, Codes and Cryptography*, 45 (2007), no. 2, 269–270.
- M. Greferath, G. McGuire, M. E. O’Sullivan, “On Plotkin Optimal Codes over Finite Frobenius Rings,” *Journal of Algebra and Its Applications*, (2006), no. 6, 799–815.
- M. Bras-Amorós, M. E. O’Sullivan, “The Correction Capability of the Berlekamp-Massey-Sakata Algorithm with Majority Voting,” *Applicable Algebra in Engineering, Communications and Computing* 17 (2006), no. 5, 315–335.
- M. E. O’Sullivan, “Algebraic Construction of Sparse Matrices with Large Girth,” *IEEE Transactions on Information Theory*, 52 (2006), no. 2, 718–727.
- M. Greferath, M. E. O’Sullivan, “On Bounds for Codes over Frobenius Rings under Homogeneous Weights,” *Discrete Mathematics* 289 (2005) pp. 11–24.
- M. E. O’Sullivan, “On Koetter’s Algorithm and the Computation of Error Values,” *Designs, Codes and Cryptography*, 31 (2004) pp. 169–188.
- M. E. O’Sullivan, “The Key Equation for One-Point Codes,” *Journal of Pure and Applied Algebra*, 169 (2002) pp. 295–320.
- M. E. O’Sullivan, “New Codes for the Berlekamp-Massey-Sakata Algorithm,” *Finite Fields and Their Applications*, 7 (2001) pp. 293–317.
- M. E. O’Sullivan, “Decoding of Hermitian Codes: The Key Equation and Efficient Error Evaluation,” *IEEE Transactions on Information Theory*, 46 (2000), no. 2, pp. 512–523.
- M. E. O’Sullivan, “Decoding of Codes Defined by a Single Point on a Curve,” *IEEE Transactions on Information Theory*, special issue on algebraic geometry codes, 41 (1995), no. 6, pp. 1709–1719.

Articles in Refereed Proceedings

- S. Lampoudi, J. Brevik, M. E. O’Sullivan, ”Combinatorial Properties as Predictors

for the Performance of the Sum-Product Algorithm,” *12th Canadian Workshop on Information Theory, (CWIT)* pp.134-138, 17-20 May 2011.

F. Hernando, M. E. O’Sullivan, E. Popovici, S. Srivastava, “Subfield-subcodes of Generalized Toric Codes,” *Proceedings IEEE International Symposium on Information Theory*, pp. 1125-1129, June 2010.

M. Bras-Amoros, M. E. O’Sullivan: “From the Euclidean Algorithm for Solving a Key Equation for Dual Reed-Solomon Codes to the Berlekamp-Massey Algorithm,” *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, M. Bras-Amoros, T. Hóholdt (eds.), Springer, Lecture Notes in Computer Science, 5527, pp. 32-42, June, 2009.

J. Brevik, M. E. O’Sullivan, A. Umlauf, R. Wolski: “Simulation of the Sum-Product Algorithm Using Stratified Sampling,” *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, M. Bras-Amoros, T. Hóholdt (eds.), Springer, Lecture Notes in Computer Science, 5527, pp. 65-72, June, 2009.

D. Monarres, M. E. O’Sullivan: “A Generalization of the Zig-zag Product by Means of the Sandwich Product,” *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, M. Bras-Amoros, T. Hóholdt (eds.), Springer, Lecture Notes in Computer Science, 5527, pp. 231-234, June, 2009.

M. Bras-Amoros, M. E. O’Sullivan: “Extended Norm-Trace Codes with Optimized Correction Capability,” *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, P. V. Kumar, T. Hóholdt, H. Janwa (eds.), Springer, Lecture Notes in Computer Science, 4851, pp. 337-346, Dec., 2007.

M. O’Sullivan, J. Brevik, R. Wolski, “The Sum-Product Algorithm on Small Graphs,” in *Advances in Coding Theory and Cryptology*, T. Shaska, W. C. Huffman, D. Joyner, V. Ustimenko eds., Series on Coding Theory and Cryptology, 2. World Scientific Publishing Co., 2007, 160–180.

E. Byrne, M. Greferath, M. E. O’Sullivan, “Duality of Ring-Linear Codes and a Linear Programming Bound,” *International Workshop on Coding and Cryptography*, Versailles, France, 2007.

R. Agarwal, E. Popovici, B. O’Flynn, M. O’Sullivan, “A Parallel Architecture for Hermitian Decoders: Satisfying Resource and Throughput Constraints,” *IEEE Proc., International Symposium on Circuits and Systems*, ISCAS 2007.

R. Moberly, M. O’Sullivan and K. Waheed, “LDPC Decoder with a Limited-Precision FPGA-based Floating-Point Multiplication Coprocessor,” *Proceedings SPIE Advanced Signal Processing Algorithms, Architectures, and Implementations*, August 2007.

R. Moberly, M. O’Sullivan, “Representing Probabilities with Limited Precision for Iterative Soft-Decision LDPC Decoding”, *Proceedings Wireless and Personal Multimedia Conference*, September 2006.

R. Moberly, M. O’Sullivan, “Computational Performance of Various Formulations of the Iterative Soft-Decision Decoder Algorithm”, *Proceedings IEEE International Symposium on Information Theory*, July 2006.

K. Lee, M. E. O’Sullivan “Groebner Bases for Soft-Decision Decoding of Reed-Solomon Codes” *2006 IEEE International Symposium on Information Theory*, Seattle, WA, July, 2006, pp. 2032–2036.

M. E. O’Sullivan, J. Brevik, R. Wolski “The Performance of LDPC codes with Large Girth,” *Proc. 43rd Allerton Conference on Communication, Control and Computing*, Univ. Illinois, 2005.

A. Byrne, E. Popovici, M. E. O’Sullivan, “Versatile Architectures for Decoding a Class of LDPC Codes,” *IEEE European Conference on Circuit Theory and Design*, 2005.

M. Greferath, M. O’Sullivan, R. Smarandache, “Construction of Good LDPC Codes Using Dilation Matrices,” *Proc. IEEE International Symposium on Information Theory*, Chicago, Illinois, p. 237, 2004.

M. E. O’Sullivan, R. Smarandache, “High-rate, Short Length, (3, 3s)-regular LDPC Codes of Girth 6 and 8,” *Proc. IEEE International Symposium on Information Theory*, Yokohama, Japan, p. 59, 2003.

M. E. O’Sullivan, M. Greferath, R. Smarandache, “Construction of LDPC Codes from Affine Permutation Matrices,” *Proc. 40th Allerton Conference on Communication, Control and Computing*, Univ. Illinois, pp. 1159-1167, 2002.

E. Popovici, P. Fitzpatrick, R. Koetter, M. E. O’Sullivan, “Implementation of a Hermitian decoder,” *Proc. IEEE Int. Symp. Information Theory*, Washington D. C., p. 311, 2001.

M. E. O’Sullivan, “Alternative Approaches to the Computation of Error Values for Hermitian Codes,” *Proc. 37th Allerton Conference on Communication, Control and Computing*, Univ. Illinois, pp. 557-566, 1999.

M. E. O’Sullivan, “Decoding of Codes on Surfaces,” *Proceedings, IEEE Information Theory Workshop*, Killarney, Ireland, pp. 33-34, 1998.

M. E. O’Sullivan, “Decoding Hermitian Codes Beyond $(d_{\min} - 1)/2$ ” *Proc. IEEE International Symposium on Information Theory*, Ulm, Germany, p. 377, 1997.

M. E. O’Sullivan, “VLSI Architecture for a Decoder for Hermitian Codes” *Proc. IEEE International Symposium on Information Theory*, Ulm, Germany, p. 376, 1997.

Short Courses

Lecturer (8 hours), Soria Summer School on Computational Mathematics: Algebraic Coding Theory, Soria, Spain, July 2-11, 2008.

Lecturer (6 hours), 2004 Summer Program for Graduate Students in Coding and Cryptography, sponsored by the Institute for Mathematics and Its Applications, University of Notre Dame, June 8-26, 2004.

Lecturer (12 hours), “Coding Theory: Code Constructions and Algorithms” Universitat Politècnica de Catalunya, Barcelona, Spain, June 2-6, 2003.

Doctoral and Post-doctoral Students Supervised

Fernando Hernando, Post-doctoral support from the Irish Research Council for Science, Engineering and Technology (IRCSET), for research at SDSU, 8/2010-8/2011.

Kwankyu Lee, Post-doctoral support from the Korea Research Foundation, for research at SDSU 8/2005-6/2006.

Raymond Moberly, *Quantization of a Low-Density Parity-Check (LDPC) Decoder: Limited Precision Digital Design of the Sum-Product Algorithm (SPA) for Wireless Voice and Video Communication Channels*, Claremont Graduate University and San Diego State University, 2012.

Maria Bras-Amorós, *Improving Evaluation Codes*, Universitat Politècnica de Catalunya, Barcelona, Spain 2003. I am co-advisor with Sebastià Xambó-Descamps.

Emanuel Popovici, *Algorithms and Architectures for Decoding Reed-Solomon and Hermitian Codes*, National University of Ireland, Cork, Ireland, 2002. I am co-advisor with Patrick Fitzpatrick.

Professional Activities and Service

TRANSFORMING POST-SECONDARY EDUCATION IN MATHEMATICS Member of the Mathematics Advisory Group, starting 1/2016.

INSTITUTE FOR MATHEMATICS AND ITS APPLICATIONS, UNIVERSITY OF MINNESOTA, General membership for the Thematic Year on Applications of Algebraic Geometry.

CONFERENCES: Co-organizer: Special Session on Coding Theory, AMS-MAA Joint Meetings, San Diego, 2002.

EDITOR: *Advances in the Mathematics of Communications*: Handled ten articles from the period 2007-2011.

REFeree: Reviewed articles for the following journals: *Advances in the Mathematics of Communications*; *Designs, Codes and Cryptography*; *Finite Fields and Their Applications*; *Journal of Pure and Applied Algebra*; *Communications in Algebra*; *Applicable Algebra in Engineering, Communication, and Computing*; *Journal of Symbolic Computation*; *IEEE Transactions on Information Theory*; *IEEE Transactions on Communications*.

MEMBERSHIPS: American Mathematical Society; Mathematical Association of America; Society of Industrial and Applied Mathematics; Institute of Electrical and Electronics Engineers—Information Theory Society.