

Michael E. O'Sullivan

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.

Research Areas: Linkage of algebraic space curves,
Generalized divisors on curves and surfaces.

Advisor: Robin Hartshorne.

Dissertation: Divisors on Normal Cubic Surfaces with Applications to the
Classification of Space Curves

M.S. MATHEMATICS: Portland State University, 1985.

B.A. MATHEMATICS: Reed College, 1981.

Employment

ASSOCIATE PROFESSOR: Department of Mathematics and Statistics, San Diego State University (6/06-present).

ASSISTANT PROFESSOR: Department of Mathematics and Statistics, San Diego State University (8/00-6/06).

Teaching and contributing to course development for a M.S. program in the mathematical theory of communications. Ongoing research in coding theory and applications of algebraic geometry.

VISITING COLLEGE LECTURER: National University of Ireland, Cork, Ireland (8/98-8/00). Supervised research projects, designed course curriculum and taught in a new M.Sc. program in information theory, coding and cryptography offered by the mathematics department. Advisor for a doctoral candidate working on the design of a VLSI implementation of a decoding algorithm.

VISITING RESEARCH ASSISTANT PROFESSOR: Coordinated Science Laboratory, University of Illinois, Urbana-Champaign (6/98-7/02). Joint research with R. Blahut and R. Kötter on implementation of algebraic geometry codes.

ASSISTANT PROFESSOR OF MATHEMATICS: University of Puerto Rico, Mayaguez (8/96-7/98). Taught courses in number theory, geometry, differential equations, and precalculus.

MATHEMATICIAN: O'Sullivan Consulting Incorporated (6/89-6/97). Conducted research on decoding of algebraic geometry codes. Developed a decoding algorithm for one-point codes, worked with hardware engineers on implementation in VLSI and with industry representatives on commercial applications.

Research Grants

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) (2/07-2/10) \$182,684. Algebraic analysis of the sum-product algorithm and experimentation using massively parallel grid computation is being used to discover the causes of decoding failure and improve code design.

KOREA RESEARCH FOUNDATION, Postdoctoral Foreign Study Grant, PI M. E. O'Sullivan (7/2005-6/2006). Support for a one-year postdoctoral position for Kwankyoo Lee. We developed a new algorithm for the interpolation step in list decoding of Reed-Solomon and Hermitian codes \$20,000.

SDSU TRAVEL GRANT, "Research Collaboration in Applied Algebra with the National University of Ireland." Two students accompanied me to a workshop in Cork, 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) (8/00-7/03). Development of practical algorithms for soft-decision decoding of Reed-Solomon and related algebraic geometry codes. 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, (7/98-6/00). Development of decoding algorithms that are well suited to hardware architecture for a broad class of codes similar to Hermitian codes. Design, fabrication and testing of a VLSI implementation.

NATIONAL SCIENCE FOUNDATION Small Business Innovations Research Grant, "Construction of a Decoder for an Algebraic Geometry Code," PI M. O'Sullivan.

Phase I (2/93-10/93). Developed a computational algorithm and computer simulation for decoding Hermitian codes.

Phase II (7/94-9/96). Incorporated improvements to the decoding algorithm into the computer simulation, oversaw hardware logic design and testing, and investigated commercial applications.

DEPARTMENT OF ENERGY Small Business Cooperative Research and Development Grant (9/94-12/94): Joint work with the Computer Research Group at the Lawrence Livermore National Laboratory on a Sisal language simulation of my decoding algorithm for the 8-bit Hermitian code. The goal was to take advantage of parallel processing for this computationally intensive algorithm.

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 Submitted to Refereed Journals

K. Lee, M. E. O'Sullivan, "Algebraic Soft-Decision Decoding of Hermitian Codes" submitted to *IEEE Transaction on Information Theory*.

K. Lee, M. E. O'Sullivan, "List Decoding of Hermitian Codes using Groebner Bases" to appear in *Journal of Symbolic Computation*.

Articles in Refereed Journals

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, 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* vol. 289 (2005) pp. 11-24.

M. E. O’Sullivan, “On Koetter’s Algorithm and the Computation of Error Values,” *Designs, Codes and Cryptography*, vol. 31 (2004) pp. 169-188.

M. E. O’Sullivan, “The Key Equation for One-Point Codes,” *Journal of Pure and Applied Algebra*, vol. 169 (2002) pp. 295-320.

M. E. O’Sullivan, “New Codes for the Berlekamp-Massey-Sakata Algorithm,” *Finite Fields and Their Applications*, vol. 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*, vol. 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, vol. 41 (1995), no. 6, pp. 1709-1719.

Articles in Refereed Proceedings

M. Bras-Amorós, M. E. O’Sullivan, “Extended Norm-Trace Codes with Optimized Correction Capability,” *Lecture Notes in Computer Science, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, P. V. Kumar, T. Höholdt, H. Janwa (eds.), Springer, vol. 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 of One-Point Codes Using Error Evaluator Polynomials,” *Proc. IEEE International Symposium on Information Theory*, Ulm, Germany, p. 384, 1997.
- 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 at the 2004 Summer Program for Graduate Students in Coding and Cryptography, sponsored by the Institute for Mathematics and Its Applications. June 8-26, 2004, University of Notre Dame.

“Coding Theory: Code Constructions and Algorithms” Universitat Politècnica de Catalunya, Barcelona, Spain, June 2-6, 2003. Delivered a 12 hour course on algebraic geometry codes, decoding and low-density parity-check codes.

Other Presentations

M. E. O’Sullivan, “Building Low-density Parity-check Codes with Affine Permutation Matrices,” 15th Annual Symposium on Mathematical Theory of Networks and Systems, Notre Dame, Aug 12-16, 2002.

M. E. O’Sullivan, “Decoding of One-Point Codes with Koetter’s Algorithm,” Conference on Symbolic Computational Algebra, London, Ontario, July, 2002.

M. E. O’Sullivan, “Construction of Codes for the Iterative Decoding Algorithm,” Conference of the Catalan Mathematical Society, Barcelona, Spain, May 2002.

M. E. O’Sullivan, “The Key Equation for One-Point Codes,” Institute for Mathematics and its Applications Summer Workshop: Codes Systems and Graphical Models, Aug. 1999.

M. E. O’Sullivan, “Decoding of Algebraic Geometry Codes,” Colloquium Lecture, University of Notre Dame, September, 1998.

M. E. O’Sullivan, “Decoding of Codes Defined by a Ring with an Order Function,” Joint Meetings of the AMS-MAA, Baltimore, Maryland, Jan., 1998.

M. E. O’Sullivan, “Decoding of One-Point Codes,” Midwest Algebraic Geometry Conference, Notre Dame, Indiana, Nov. 1997.

M. E. O’Sullivan, “The Key Equation for One-Point Codes,” Workshop on Arithmetic, Geometry and Coding Theory, Luminy, France, June 1997.

M. E. O’Sullivan, “Classification and Divisor Class Groups of Normal Cubic Surfaces in \mathbf{P}^3 ” Eastern Section meeting of the American Mathematical Society, Oct 5, 1996.

Doctoral Students Supervised

Raymond Moberly, Doctoral Candidate, Computational Sciences, San Diego State University and Claremont Graduate University.

Maria Bras-Amorós, *Improving Evaluation Codes*, Universitat Politècnica de Catalunya, Barcelona, Spain 2003. 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. Co-advisor with Patrick Fitzpatrick.

Professional Activities and Service

INSTITUTE FOR MATHEMATICS AND ITS APPLICATIONS, UNIVERSITY OF MINNESOTA, general membership for the Thematic Year on Applications of Algebraic Geometry. I spent 15 weeks at the Institute and attended several workshops.

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

REFEREE: Reviewed articles for the following journals.

- *Designs, Codes and Cryptography*;
- *IEEE Transactions on Information Theory*;
- *Finite Fields and Their Applications*;
- *Applicable Algebra in Engineering, Communication, and Computing*.

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

EDUCATION: Served on San Diego City Schools' K-5 Textbook Adoption Committee, 2001-2002.

Miscellaneous CITIZENSHIP: United States, Ireland.

FOREIGN LANGUAGES: French, Spanish.

PEACE CORPS VOLUNTEER: Taught mathematics for two years at a lycée in the Central African Republic (6/86-6/88).