Magnus Gausdal Find

Contact Information

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive, Gaithersburg, Maryland, USA
Private contact information:
12504 Village Square Terrace, Apt. 202
Rockville, Maryland, 20852
USA

magnus.find@nist.gov
magnusgfind.wordpress.com

About Me

28 years old. Born and raised in Denmark. Currently based in Maryland, USA. Until recently I was a PhD student at University of Southern Denmark under the supervision of Joan Boyar. My research is generally within cryptography and computational complexity, especially cryptographic complexity measures. When I don't work, I like to run and play music. I sing and play the guitar.

Main Research Interests

Most of my research is within the area of circuit complexity and cryptographic nonlinearity measures, specifically studying relationships between different nonlinearity criteria, with particular focus on multiplicative complexity, and the computational complexity of computing such measures. I have also done research on the structure of the computation of linear operators.
Besides that I have a general interest in cryptography, computational complexity, and algorithms.

Post Doctoral Experience

University of Southern Denmark: Instructor, Combinatorial Mathematics, Feb 2015 to May 2015

- Responsible for teaching the course "Combinatorial Mathematics"

National Institute of Standards and Technology: Research Associate, May 2015 to present

- Research associate in the *Cryptographic Technology Group*. Most of my work is within either circuit minimization or the relation between multiplicative complexity and cryptographic properties

Education

University of Southern Denmark, Odense, Denmark

Ph.D., Computer Science, Feb 2011 to Feb 2015

- Thesis Topic: *Linearity and Nonlinearity: Complexity and Measures*
- Advisor: Joan Boyar, Ph.D

MSc. Scient., Computer Science with Profile in Research, 2009-2012

BSc. Scient., Computer Science with minor in Mathematics, 2006-2010

- Bachelor's Thesis Topic: *Algorithms for Quantum Computers*. Available via my home page. Has subsequently been used in a course on quantum algorithms by Francois Schwarzentreuber.

Peer Reviewed Journal Publications

1. Joan Boyar and Magnus Gausdal Find. Cancellation-free circuits in unbounded and bounded depth. *Theor. Comput. Sci.*, 590:17–26, 2015.
2. Joan Boyar, Magnus Gausdal Find, and René Peralta. On various nonlinearity measures for boolean functions. *Cryptography and Communications*, 2015. To appear.

Peer Reviewed Conference Publications

1. Joan Boyar, Magnus Find, and René Peralta. Four measures of nonlinearity. In Paul G. Spirakis and Maria J. Serna, editors, *CIAC*, volume 7878 of *Lecture Notes in Computer Science*, pages 61–72. Springer, 2013.
2. Joan Boyar and Magnus Gausdal Find. Cancellation-free circuits in unbounded and bounded depth. In Leszek Gasieniec and Frank Wolter, editors, *FCT*, volume 8070 of *Lecture Notes in Computer Science*, pages 159–170. Springer, 2013.
3. Joan Boyar and Magnus Gausdal Find. The relationship between multiplicative complexity and nonlinearity. In Ersébet Csuhaj-Varjú, Martin Dietzfelbinger, and Zoltán Ésik, editors, *MFCS*, volume 8635 of *Lecture Notes In Computer Science*, pages 130–140. Springer, 2014.
4. Magnus Gausdal Find. On the complexity of computing two nonlinearity measures. In Edward A. Hirsch, Sergei O. Kuznetsov, Jean-Éric Pin, and Nikolay K. Vereshchagin, editors, *Computer Science - Theory and Applications - 9th International Computer Science Symposium in Russia, CSR 2014, Moscow, Russia, June 7-11, 2014. Proceedings*, volume 8476 of *Lecture Notes in Computer Science*, pages 167–175. Springer, 2014.

Journal Publications in Submission

1. Magnus Find, Mika Göös, Matti Järvisalo, Petteri Kaski, Mikko Koivisto, and Janne H. Korhonen. Separating OR, SUM, and XOR circuits. October 2013. In submission.
2. Magnus Gausdal Find and Joan Boyar. On various nonlinearity measures for boolean functions. July 2015. In submission.
3. Magnus Gausdal Find, Meltem Soönmez Turan, and Daniel Smith-Tone. The number of boolean functions with multiplicative complexity 2. August 2015. In submission.

Conference Talks

- *Cancellation-free circuits: An approach for proving superlinear lower bounds for linear Boolean operators*, at CiE 2012, Computability in Europe: Turing Centenary Conference. Cambridge, United Kingdom, June 2012
- *Four Measures of Nonlinearity*, at CIAC'2013 (8th International Conference on Algorithms and Complexity). Barcelona, Spain. May 2013
- *On Cancellation-Free Linear Circuits*, at CTW'2013 (China Theory Week). Aarhus, Denmark. July 2013
- *Cancellation-Free Circuits in Unbounded and Bounded Depth*, at FCT'2013 (19th International Symposium on Fundamentals of Computation Theory). Liverpool, United Kingdom. August 2013
- *On The Complexity of Computing Two Nonlineraity Measures*, at CSR'2014 (9th International Computer Science Symposium in Russia). Moscow, Russia. June 2014
- *The Relationship Between Multiplicative Complexity and Nonlinearity*, at MFCS'2014 (39th International Symposium on Mathematical Foundations of Computer Science). Budapest, Hungary. August 2014

Other Academic Activities

Talk *Trade-off between Multiplicative and Gate Complexity*, at ARCO Workshop (Algorithmic Research: Cooperation around Oresound). Uni. of Copenhagen, Copenhagen, Denmark. April 2012

Talk *On Computing the Multiplicative Complexity*, at Uni. of Aarhus Crypto Seminar. Uni. of Aarhus, Aarhus, Denmark. February, 2014

Talk *The Relationship Between Multiplicative Complexity and Nonlinearity*, Crypto Seminar National Institute of Standards and Technology, Gaithersburg, Maryland, USA. July, 2014

Visitor Visited Prof. Toniann Pitassi at the University of Toronto in the fall 2012. Toronto, Canada. August-December 2012

Participant *Madalgo and CTIC Summer school on high dimensional geometric computing*,

Participant *Workshop on Algebraic Complexity Theory* Uni. of Aarhus, Aarhus, Denmark. March, 2013

Participant *Swedish Summer School in Computer Science* (arranged by KTH, Stockholm), Stockholm archipelago, Sweden. June 2014

Participant *ICALP'2014 (41st Internation Colloquium on Automata, Languages, and Programming)*, IT University of Copenhagen, Copenhagen, Denmark. July 2014

Reviewer External Reviewer for *LATIN'14* (Latin American Theoretical INformatics Symposium), *ICALP'15* (International Colloquium on Automata, Languages, and Programming), *SAC'15* (Selected Areas in Cryptography), *MILCOM'15* (Premier International Conference for Military Communications)

Teaching Experience

Since 2008 I have had teaching responsibilities, for the Department of Mathematics and Computer Science, University of Southern Denmark. I have teaching experience in many different subjects, including programming, statistics, algorithms, and discrete mathematics. I like teaching, and usually receive excellent evaluations. In the list below, TA is short for "teaching assistant".

TA Fall 2008: Introduction to Java Programming (Instructor: Martin Ehmsen)

TA Spring 2009: Algorithms and Data Structures (Instructor: Lene Monrad

Favrholt)

TA	Fall 2009: Introduction to Java Programming (Instructor: Martin Ehmsen), Combinatorics, Probabilities and Randomized Algorithms (Instructor: Jørgen Bang-Jensen)
TA	Spring 2010: Algorithms and Complexity (Instructor: Joan Boyar), Science Statistics (Instructor: Bent Jørgensen)
TA	Fall 2010: Mathematical Tools for Computer Science (Instructor: Daniel Merkle), Combinatorics, Probabilities and Randomized Algorithms (Instructor: Jørgen Bang-Jensen)
TA	Spring 2011: Algorithms and Complexity (Instructor: Joan Boyar), Science Statistics (Instructor: Bent Jørgensen)
TA	Fall 2011: Introduction to Computer Science (Instructor: Joan Boyar)
TA	Spring 2012: Algorithms and Complexity (Instructor: Joan Boyar)
TA	Fall 2013: Introduction to Computer Science (Instructor: Joan Boyar)
Project Supervisor	Spring 2014: Supervising two group projects for first year computer science students in a project on "Digital Signatures". This included meeting with the students, helping defining the content, grading a report and conducting an oral exam defending their report.
Course Instructor	I was instructor and teaching assistant in the course *Combinatorial Mathematics*. Responsible for selection of topics and litterature, timetable planning, conducting and planning exams and written assignments.

Other Activities

- 2008 - 2010: Chairman of the Student Association of the Department of Mathematics and Computer Science.
- 2008 - 2010: "Ambassador" of University of Southern Denmark. I was a part in everything related to outreach to potential students, e.g. giving talks at at events, arranged presentations of the department, etc.
- 2011 - 2015: Member of the department's PhD committee