

JOHAN S. H. ROSENKILDE, NÉ NIELSEN

RESEARCH INTERESTS

Algebraic and Algorithmic aspects of Computer Science, Discrete Mathematics and Engineering.
Specialised in Algebraic Coding Theory using Algebraic Geometry and Computer Algebra.

RESEARCH POSITIONS

- Sep 2015 – Assistant Professor in Applied Algebra at [Technical University of Denmark](#) (DTU)
At Department of Applied Mathematics and Computer Science
- Oct 2014 – Postdoctoral Researcher at [INRIA Saclay-Ile-de-France](#), on Ecole Polytechnique
Aug 2015 *In Team Grace, headed by Senior Researcher Daniel Augot.*
Project title: “Coppersmith’s methods for coding theory”
- Aug 2013 – Postdoctoral Researcher at [Universität Ulm](#), Germany
Oct 2014 *At Institute of Communications Engineering, headed by Professor Martin Bossert.*
Research in algebraic coding theory and applications.

PROJECTS

- (2016–2018) [Supervisor for H.C. Ørsted-COFUND Postdoc Vincent Neiger](#)
Title: Structured polynomial linear algebra and applications to decoding algorithms
- 2014 – 2016 [Technical Manager for Research-Based Software Development](#)
Title: Algorithmic Coding Theory in Sage
Implement framework and algorithms for experimental research in algebraic coding theory.
Employs a full-time software developer. Co-managed with Daniel Augot and Clément Pernet. funded by INRIA.
Website: bitbucket.org/lucasdavid/sage_coding_project

EDUCATION

- 2010 – 2013 Ph.D. in Mathematics, [DTU](#)
Project title: “List Decoding of Algebraic Codes”. Developed a framework based on computer algebra methods for efficient realisation of all decoding principles for Reed–Solomon codes, setting several new speed records. Applied the same principles to Algebraic Geometry codes. Available at jsrn.dk/downloads/jsrn_thesis.pdf.
- 2012 5 months research stay at [INRIA Saclay-Ile-de-France](#) on Ecole Polytechnique
Visiting Senior Researcher Daniel Augot and Team Grace
- 2009 – 2013 [Participation in doctorate schools on algebraic geometry and number theory](#)
- | | | |
|------|--|--------------------------|
| 2013 | <i>Quadratic Forms, Lattices and Applications</i> | <i>CUSO, Switzerland</i> |
| 2011 | <i>Effective Aspects of Algebra and Number Theory</i> | <i>4th ACAGM Belgium</i> |
| 2010 | <i>Algebraic Geometric Modelling in Information Theory</i> | <i>3rd ACAGM Spain</i> |
| 2009 | <i>Applied Computational Algebraic Geometric Modelling</i> | <i>2nd ACAGM Spain</i> |
- 2007 – 2010 M.Sc. Engineering in Informatics, [DTU](#)
GPA: 11.9 (7-scale, grades from –3 to 12)
- 2004 – 2007 B.Sc. in Software Technology, [DTU](#)
GPA: 10.8 (7-scale, grades from –3 to 12)

INTERNATIONAL RELATIONS

- Invited by: Dagstuhl, Luminy, ENS Lyon, U. Waterloo, Fields, Rennes U1, Inria, Ulm U., AAU, ao.
Co-author nationalities: France, Germany, Canada, China, Russia, Egypt, Netherlands, Denmark
- 2016 1 months research stay at [U. Waterloo](#), Canada
- 2015 3 weeks research visit at [U. Waterloo](#) and [U. Western Ontario](#), Canada
- 2012 5 months research stay at [Inria Saclay-Ile-de-France](#) on Ecole Polytechnique.

 ACCOMPLISHMENTS

- 2013 Participated in the [Heidelberg Laureate Forum 2013](#).
Exceptional math and CS workshop modelled over the Lindau meetings: award-winning researchers are invited along with selected PhD and postdocs.
- 2012 Awarded travelling grant by the [Idella Foundation](#), 30.000 kr.
Based on motivated application following nomination by DTU Mathematics
- 2012 Awarded travelling grant by the [Otto Mønsted Foundation](#), 20.000 kr.
Based on motivated application
- 2011 Among [Top-10 Teaching Assistants of the Year](#) at DTU.
Awarded by the student magazine Krydsfelt by recommendation from students. During the course “Differential Equations and Infinite Series”
- 2009 Received the “[IT-Student of the Year 2009](#)” award along with 10.000 kr. prize.
Netcompany acted as judge for the award, which was given at Universum Awards.
- 2009 The article “[A Behavioral Synthesis Frontend to the Haste/TiDE design flow](#)” finalist for “[Best paper award](#)” at the ASYNC 2009 Conference.
- 2002–2003 Competes in international science olympiads for youths.
Qualifies by being finalist in the national competitions of each subject.
- [International Mathematics Olympiad](#) in Tokyo.
 - [International Olympiad in Informatics](#) in Wisconsin.
 - [International Physics Olympiad](#) in Taiwan, qualifies but cannot attend.

 PEER-REVIEWED JOURNAL PUBLICATIONS

(†): The authors for this article are sorted alphabetically

- 2016 [Row Reduction Applied to Decoding of Rank Metric and Subspace Codes](#)
*Sven Puchinger, **Johan Rosenkilde né Nielsen**, Wenhui Li and Vladimir Sidorenko*
Designs, Codes and Cryptography. Online doi: [10.1109/TIT.2015.2424415](https://doi.org/10.1109/TIT.2015.2424415)
- 2015 [Sub-quadratic Decoding of One-point Hermitian Codes](#)
Johan S. R. Nielsen and Peter Beelen
IEEE Trans. Information Theory, vol. 61 (6), pp 3225–3240.
doi: [10.1109/TIT.2015.2424415](https://doi.org/10.1109/TIT.2015.2424415)
- 2014 [Multi-Trial Guruswami–Sudan Decoding for Generalised Reed–Solomon Codes](#)
Johan S. R. Nielsen and Alexander Zeh
Designs, Codes and Cryptography, 73 (2), pp 507–527. doi: [10.1007/s10623-014-9951-7](https://doi.org/10.1007/s10623-014-9951-7)
- 2013 [On the Wu List Decoder and List-Decoding Binary Goppa Codes](#)
 (†) Peter Beelen, Tom Høholdt, **Johan S. R. Nielsen**, and Yingquan Wu.
IEEE Trans. Information Theory, 59 (6), pp 3269–3281. doi: [10.1109/TIT.2013.2243800](https://doi.org/10.1109/TIT.2013.2243800)

 PEER-REVIEWED CONFERENCE PUBLICATIONS

- 2016 [Algorithms for Simultaneous Padé Approximations](#)
Johan Rosenkilde né Nielsen, Arne Storjohann
International Symposium in Symbolic and Algebraic Computation
- 2015 [Solving Shift Register Problems over Skew Polynomial Rings using Module Minimization](#)
 (†) Wenhui Li, **Johan S. R. Nielsen**, Sven Puchinger, Vladimir Sidorenko
International Workshop on Coding and Cryptography 2015
- 2014 [Power Decoding of Reed–Solomon Codes Revisited](#)
Johan S. R. Nielsen
Proc. International Castle Meeting on Coding Theory and Applications 2014
- 2014 [Fast Kötter–Nielsen–Høholdt Interpolation in the Guruswami–Sudan Algorithm](#)
Johan S. R. Nielsen
Proc. International Workshop on Algebraic and Combinatoric Coding Theory 2014
- 2014 [Power Decoding Reed–Solomon Codes up to the Johnson Radius](#)
Johan S. R. Nielsen
Proc. International Workshop on Algebraic and Combinatoric Coding Theory 2014

- 2014 [Reduced List-Decoding of Reed–Solomon Codes Using Reliability Information](#)
Mostafa H. Mohamed, **Johan S. R. Nielsen**, Martin Bossert
Proc. International Symposium on Mathematical Theory of Networks and Systems 2014
- 2013 [Generalised Multi-sequence Shift-Register Synthesis using Module Minimisation](#)
Johan S. R. Nielsen
Proc. IEEE Intl. Symp. on Information Theory 2013. doi: [10.1109/ISIT.2013.6620353](https://doi.org/10.1109/ISIT.2013.6620353)
- 2013 [On Decoding Interleaved Chinese Remainder Codes](#)
Wenhui Li, Vladimir Sidorenko and **Johan S. R. Nielsen**
Proc. IEEE Intl. Symp. on Information Theory 2013. doi: [10.1109/ISIT.2013.6620387](https://doi.org/10.1109/ISIT.2013.6620387)
- 2013 [Multi-Trial Guruswami–Sudan Decoding for Generalised Reed–Solomon Codes](#)
Johan S. R. Nielsen and Alexander Zeh
Proc. International Workshop on Coding and Cryptography 2013
- 2009 [Behavioral Synthesis Frontend to the Haste/TiDE design flow](#)
Sune F. Nielsen, Jens Sparsø, Jonas B. Jensen and **Johan S. R. Nielsen**
Proc. ASYNC 2009. doi: [10.1109/ASYNC.2009.10](https://doi.org/10.1109/ASYNC.2009.10). Finalist for Best Paper Award.

PUBLISHED OPEN SOURCE SOFTWARE

- 2016 [Google Summer of Code Mentor](#)
Project for Rank-Metric codes in SageMath
- 2010 – [SageMath Developer](#)
Involved in more than 90 improvements.
Co-designer of the Coding Theory framework in SageMath
- 2012 – [Codinglib: a toolbox for algebraic coding theory](#)
Collection of asymptotically fast algorithms for algebraic coding theory for SageMath
Including list-decoding of Reed–Solomon and One-Point Hermitian codes.
On-going project. Website: jsrn.dk/codinglib

TEACHING AND SUPERVISION

- Course Responsible: 3 courses (1 Master’s level, 5 ECTS. 2 Bachelor’s level, 5 ECTS)
- Bachelor’s thesis: 3 co-advised (1 Ulm University, 2 DTU)
- Master’s thesis: 1 co-advised (DTU)

INVITED TALKS

- 2016 [SageMath for research and teaching in Coding Theory](#)
[Dagstuhl seminar: Coding Theory in the time of Big Data](#) 30 min. 2016-08-11
- 2015 [Polynomial Approximation Problems in Algebraic Coding Theory](#)
[East Coast Computer Algebra Day 2015](#) 50 min. 2015-10-03
[Symbolic Computation Group, University of Waterloo, Canada](#) 50 min. 2015-06-26
[University of Western Ontario, Canada](#) 50 min. 2015-06-24
- 2015 [Power Decoding Reed-Solomon Codes Up to the Johnson Radius](#)
[Séminaire Codage, Cryptologie, Algorithmes, Telecom Paris](#) 40 min. 2015-06-12
- 2015 [Power Decoding of Hermitian codes in Sub-Quadratic Time](#)
[AGCT15, Luminy, Marseilles](#) 20 min. 2015-05-19
[Séminaire de GTBAC, Télécom ParisTech, France](#) 50 min. 2015-03-10
[Université de Rennes, France](#) 50 min. 2015-01-09
- 2014 [Fast Decoding of Hermitian Codes using Lattice Basis Reduction](#)
[Day on Codes, Lattices, Ideals, Cryptography, UVSQ Versailles](#) 50 min. 2014-12-10
- 2014 [Finding Bivariate Polynomials with Prescribed Zeroes:](#)
An Example of Optimisation Techniques in Computational Algebra
[Mathematics Colloquium at DTU](#) 45 min. 2014-09-03
- 2014 [2D Padé Approximations: the What, Why and Hows](#)
[ENS de Lyon, France](#) 45 min. 2014-02-13
- 2014 [Fast List-Decoding of Hermitian Codes](#)
[INRIA Saclay-Ile-de-France, France](#) 50 min. 2012-10-12

2013	Approximating Power Series Using Small Rational Expressions Mathematics Colloquium at DTU	<i>20 min. 2013-05-08</i>
2013	Multi-trial Guruswami-Sudan Decoding for Generalised Reed-Solomon Codes East China Normal University, China	<i>25 min. 2013-04-08</i>
2012	The Wu List Decoding Algorithm INRIA Rocquencourt, France	<i>30 min. 2012-12-06</i>
2012	List Decoding and the Wu Algorithm Luminy Aix-Marseilles, France	<i>45 min. 2012-11-22</i>
2012	The Wu List Decoder for Reed-Solomon Codes, Using the Euclidean Algorithm East China Normal University, China Ulm University, Germany INRIA Saclay-Ile-de-France, France Aalborg University, Denmark	<i>25 min. 2012-05-27</i> <i>50 min. 2012-11-17</i> <i>30 min. 2012-01-23</i> <i>30 min. 2011-12-06</i>

CONFERENCE TALKS

Presentations for articles in the conference proceedings. Article and talk have the same name.

2016	Algorithms for Simultaneous Padé Approximation Int'l Symposium in Symbolic and Algebraic Computation.	<i>20 min. 2016-07-22</i>
2014	Power Decoding of Reed–Solomon Codes Revisited Intl. Castle Meeting on Coding Theory and Applications	<i>2014-09 15–18</i>
2014	Fast Kötter–Nielsen–Høholdt Interpolation in the Guruswami–Sudan Algorithm Intl. Workshop on Algebraic and Combinatoric Coding Theory	<i>2014-09 09–13</i>
2014	Power Decoding Reed–Solomon Codes up to the Johnson Radius Intl. Workshop on Algebraic and Combinatoric Coding Theory	<i>2014-09 09–13</i>
2013	Generalised Multi-sequence Shift-Register Synthesis using Module Minimisation IEEE Intl. Symposium on Information Theory	<i>2013-07 07–13</i>
2013	Multi-Trial Guruswami–Sudan Decoding for Generalised Reed–Solomon Codes International Workshop on Coding and Cryptography	<i>2013-04 15–19</i>

SERVICE TO PROFESSION

Journal submissions reviewed for (article count in parentheses):

IEEE Trans. Information Theory	(3)	IEEE Trans. Comm. Theory	(3)
Designs, Codes and Cryptography	(4)	Intl. J. Computer Mathematics	(1)
Discrete Math.	(1)	Th. Comp. Science	(1)
Adv. Mathematics of Communication	(4)		

Conference submissions reviewed for:

ACM-SIAM Symp. Discrete Math.	(1)	C2SI	(1)
ANTS	(2)	ISSAC	(1)
Intl. Symp. Information Theory	(4)	Intl. Wksp. Coding and Cryptography	(3)

LANGUAGES

Danish	Mother tongue	French	Intermediate fluency
English	Fluent	German	Basic level