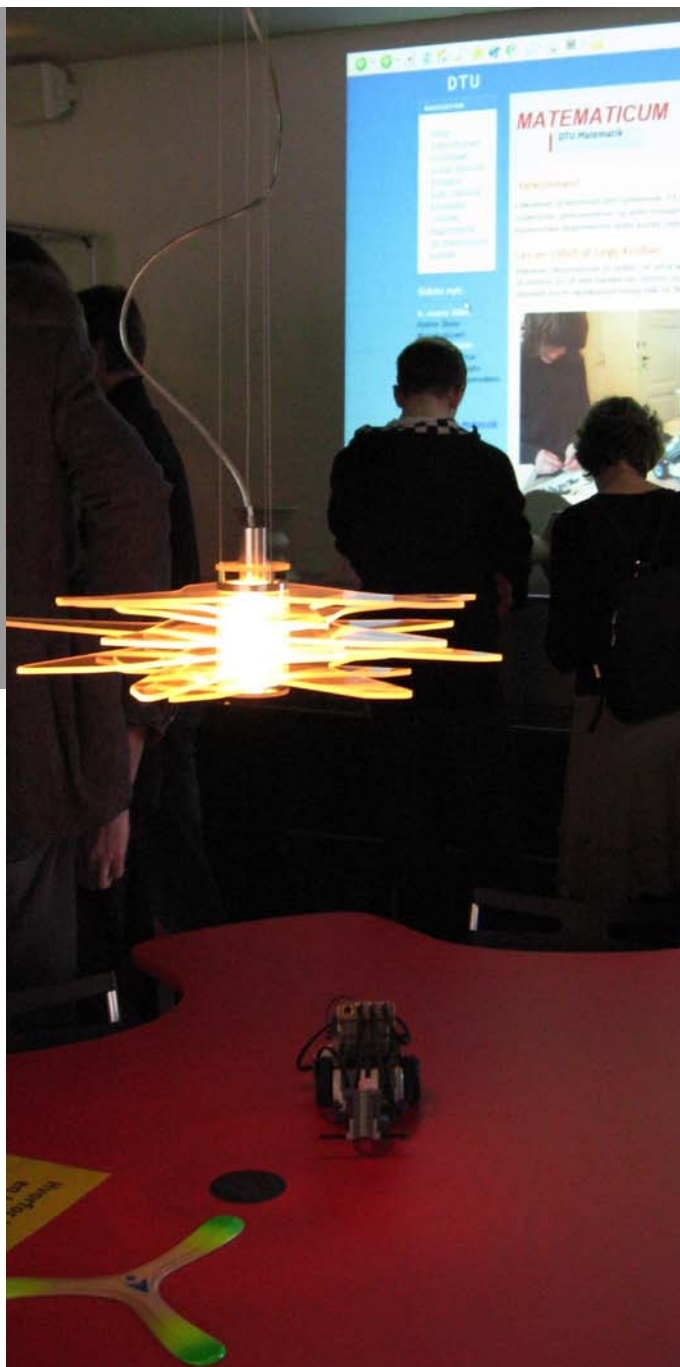


# Annual Report 2010



**DTU Mathematics**  
Department of Mathematics

---



The Enigma encryption machine from 1942 from Matematicum

Annual Report 2010  
MAT – Department of Mathematics ©  
Technical University of Denmark  
Matematiktorvet B. 303S  
Dk-2800 Kgs. Lyngby, Denmark  
[www.mat.dtu.dk](http://www.mat.dtu.dk)

## PREFACE

This document contains a detailed reporting on the activities of the Department of Mathematics (DTU Mathematics), Technical University of Denmark (DTU), for the calendar year 2010. The reporting is primarily focused on the research related tasks of our department.

Highlights and dominating events and achievements for 2010 include:

- The cryptology group is behind a cryptographic system which is on the shortlist of a competition to become a standard American government system.
- Ole Christensen was appointed full professor in Applied Functional Analysis.
- Poul Hjorth was appointed “Teacher of the year” at DTU.
- The bachelor programme “Matematik og Teknologi” has received an increasing number of students.
- DTU-Mathematics has established a formal cooperation with KAIST, Korea.
- A Danish-Chinese research center for Coding Theory headed by Tom Høholdt was funded by “Danmarks Grundforskningsfond” (with start 2011).
- 7 new Ph.D-students have been enrolled.
- New teaching material for the large courses Matematik 1 and Diplommat 1+2 is introduced.

**Michael Pedersen**  
Head of Department

March, 2011

## CONTENTS

1.	Preface .....	3
2.	Staff.....	5
3.	Research.....	7
4.	Research publications .....	28
5.	Research collaboration.....	36
6.	Conference participation.....	40
7.	Research presentations outside DTU Mathematics.....	43
8.	Teaching activities .....	44
9.	Research related tasks .....	47
10.	Popularizing Science.....	51
11.	Other information .....	52

## Advisory Board

The department's Advisory Board consists of 5 external representatives of the department's core interests. The members of the board are appointed by the Head of Department. Their main task is to provide consultancy about the activities of the department in the areas of education, research and innovation.

*Members of the Advisory Board in 2010 are:*

Thomas Jakobsen  
Havok, The Digital Depot  
Dublin, Ireland

Senior Associate Professor Magnus Fontes  
Matematikcentrum  
Lund University, Sweden

Department Head Steen Ingwersen  
Novo Nordisk A/S  
Søborg, Denmark

Professor Eva B. Vedel Jensen  
Aarhus University  
Institute for Mathematics  
Aarhus, Denmark

Academic Advisor Bjørn Grøn  
Ministry of Education  
Copenhagen, Denmark

## Annual report 2010

### DTU Mathematics Department of Mathematics

---

#### 1. Basic Data

Technical University of Denmark  
Matematiktorvet  
Building 303S  
DK-2800 Kgs. Lyngby, Denmark  
Tel: +45 -45 25 30 31  
Fax: +45- 45 88 13 99  
Web: www.mat.dtu.dk

#### Head of department

Professor, dr. techn. Michael Pedersen

#### Personnel as of 01.12.2010

5 Professors  
3 Professors (Docents)  
13 Associate professors (lektor)  
3 Assistant professors (adjunkt)  
3 Postdocs  
16 Ph.D. students  
8 Technical and administrative staff

#### 2. Staff

##### 2.1 Faculty

*Alsholm*, Preben Kjeld, Ph.D., lektor  
*Beelen*, Peter, Ph.D., lektor  
*Brander*, David, Ph.D., lektor, (4 mths. from 1.9.10, adjunkt 8 mths. to 31.8.10)  
*Brøns*, Morten, lic. techn., professor  
*Christensen*, Ole, dr. scient., professor, (7 mths. from 1.6.10, docent 5 mths. to 31.5.10)  
*Evgrafov*, Anton, Ph.D., lektor, (3 mths. from 1.10.10, adjunkt 9 mths. to 30.9.10)  
*Gravesen*, Jens, D. Phil., lektor  
*Hansen Vagn Lundsgaard*, Ph.D., professor (9 mths. to 30.9.10)

*Henriksen*, Christian, Ph.D., lektor  
*Hjorth*, Poul G., Ph.D., lektor  
*Høholdt*, Tom, cand. scient., docent  
*Knudsen*, Kim, Ph.D., lektor  
*Knudsen*, Lars Ramkilde, Ph.D., professor  
*Larsen*, Inger, cand. scient., docent  
*Leander*, Gregor, Ph.D., lektor,  
*Markvorsen*, Steen, lic. techn., professor  
*Pedersen*, Michael, Ph.D., dr. techn, professor  
*Røgen*, Peter, Ph.D., lektor  
*Skovgaard*, Ove, lic. techn., docent  
*Starke*, Jens, Dr. rer. nat., lektor  
*Stolpe*, Mathias, tekn. dr., lektor  
*Sørensen*, Mads Peter, lic. techn., lektor  
*Thomassen*, Carsten, Ph.D., professor  
*Zenner*, Erik, Dr. rer. nat., adjunkt  
*Thomsen*, Søren Steffen, Ph.D., adjunkt (from 01.03.2010)

##### 2.2. Research staff (With indication of funding<sup>1</sup>)

*Bogomolny*, Michael, Ph.D., forsker, (4 mths. to 30.4.10, FTP)  
*Chamoun*, George Chaouki, postdoc (8 mths. to 31.8.10, Hans Christian Ørsted postdoc programme)  
*Finnerup*, Bodil, videnskabelig assistent, (1 mth. to 31.1.10)  
*Gauravaram*, Praveen, Ph.D. postdoc (FTP)  
*Gregersen*, Misha Marie, Ph.D. postdoc (EU FlowHEAD)  
*Marhadi*, Kun Saptohartyadi, postdoc., (11 mths. from 1.2.10, Villum Kann Rasmussen Fonden)  
*Matusiewicz*, Krystian, Ph.D., postdoc (1,5 mth to 17.2.10, FTP)  
*Munoz*, Eduardo, videnskabelig assistent, (2 mths. to 31.8.10)  
*Schilder*, Frank, Ph.D., adjunkt  
*Thomsen*, Søren Steffen, Ph.D., postdoc (Villum Kann Rasmussen Fonden; until 28.02.2010)

##### 2.3 Teaching staff

*Andersen*, Leif, cand.scient, ekstern lektor, (4 mths. from 1.9.10)  
*Hoffmann*, Peter, cand. scient, ekstern lektor

---

1) FNU: Danish Natural Science Research Council  
FTP: Danish Research Council for Technology and Production Sciences  
FUU: Researcher education, Danish Agency for Science, Technology and Innovation.

## Annual Report 2010 – Department of Mathematics DTU

*Jensen*, Helge Elbrønd, cand. scient. (4 mths. from 1.9.10)

*Jensen*, Mogens Tønsberg, cand.scient., (4 mths. from 1.9.10)

*Lund*, Michael, cand.scient., (4 mths. from 1.9.10)

*Pedersen*, Ulrik Engelund, cand.scient., (4 mths. from 1.9.10)

*Petersen*, Petur Birgir, cand.scient., (4 mths. from 1.9.10)

*Schmidt*, Karsten, cand.mag., (4 mths. from 1.9.10)

### 2.4 Ph.D. students

*Abdelraheem*, Mohamed Ahmed, (inst.stip.)

*Alkhezaimi*, Hoda, 1,5 mth. from 15.11.10, (Emirates Advanced Investments)

*Amir*, Oded, (DTU-stip.)

*Andersen*, Morten, (5 mths. from 1.8.10, inst.stip.)

*Andersen*, Nina Marianne (7 mths. to 31.7.10, Novo Nordisk A/S)

*Borghoff*, Julia (FTP)

*Brander*, Kristian (1 mth. to 31.1.10, DTU-stip.)

*Duun*, Marie Bro, (DTU-stip.)

*Elmegård*, Michael, (inst.stip.)

*Munoz*, Eduardo (5 mths. to 31.5.10, FTP)

*Nguyen*, Dang Manh, (inst.stip.)

*Nielsen*, Johan Sebastian Rosenkilde, (6 mths. from 1.7.10, inst.stip.)

*Nielsen*, Peter Nørtoft, (inst.stip.)

*Pedersen*, Johan Rønby, (1/2 Danmarks Grundforskningsfond, 1/2 inst.stip.)

*Pedersen*, Louis, (Greenwood Engineering A/S)

*Rasmussen*, Marie-Louise Højlund (2,5 mths. to 12.3.10, DTU-stip.)

*Umana*, Valerie Gauthier, (Villum Kann Rasmussen Foundation)

*Vinther*, Frank, (9 mths. from 1.4.10, 1/2 FTP, 1/2 DTU Matematik)

*Weldeyesus*, Alemseged Gebrehiwot, (0,5 mth. from 15.12.10, FUU)

*Zermeno*, Victor Manuel Rodriguez, (1/3 Vestas A/S, 1/3 FUU, 1/3 inst.stip.)

*Zhang*, Lai, (1/3 globaliseringsmidler, 1/3 DTU Aqua, 1/3 inst.stip.)

### 2.5.1 Guest professors

*Aldred*, R.E.L. Professor, University of Otago, Dunedin, New Zealand, October 4-November 27, 2010. Funded by own university. Accommodation paid by FNU grant "Forskningsbevilling til Diskret Matematik".

*Bassa*, Alp, Doctor, CWE, Amsterdam, The Netherlands, May 31-June 13, 2010.

*Beltrán*, Alberto, Universidad Nacional Autónoma de México, June 31-July 6, 2010 (DCAMM).

*Ghorpade*, Sudhir Ramakant, Indian Institute of Science, April 26-July 17, Otto Mønsted Fond

*Efendiev*, Messoud, Dept. of Dynamical Systems, Inst. of Biomathematics and Biometry, Helmholtz Zentrum München, Germany, May 6-8 and August 3-17, 2010.

*Eiswirth*, Markus, Fritz Haber Institut, Berlin, Germany, January 5-9, 2010.

*Gaididei*, Yuri B., professor, Bogolyubov Institute of Theoretical Physics, Kiev, Ukraine, May 25-June 25 and September 1-15, 2010.

*Gorria*, Carlos, Dr., University of the Basque Country, Bilbao, Spain, May 24-June 4, 2010 (own funding).

*Hurtado*, Ana, University of Granada, Spain, May 2-15, 2010.

*Janwa*, H., University of Puerto Rico, Puerto Rico, USA., July 25-August 14, 2010.

*Kim*, Rae Young, Professor, Yeungnam University, Korea, July 27-August 10, 2010.

*Knobloch*, Edgar, University of California, Berkeley, March 22-30, 2010 (Fluid.DTU)

*Krauskopf*, Bernd, University of Bristol, UK, December 10-14, 2010.

*Kündgen*, André, Associate Professor, California State University San Marcos, May 3-June 30, 2010. Funded by own university. Accommodation paid by "FNU forskningsbevilling til diskret matematik".

*Matano*, Hiroshi, University of Tokyo, Japan, September 10-14, 2010.

*Melbourne*, Ian, University of Surrey, Guildford, UK, April 8-11, 2010.

*Ohnishi*, Isamu, University of Hiroshima, Japan, May 28-29, 2010.

*Palmer*, Vincente, Universitat Jaume I, Castellon, Spain, May 2-8, 2010 and July 27-August 8, 2010.

*Powell*, Alex, Assistant Professor, Vanderbilt, USA, May 28-June 7, 2010.

*Reichert*, Christian, Institut Nationale des Sciences Appliquées (INSA) at Lyon, France, January 5-9, 2010.

*Sieber*, Jan, University of Portsmouth, UK, January 28-February 2, 2010.

*Stoeva*, D., University of Sofia, Bulgaria, September 10-17, 2010.

*Thorup*, M., Research Fellow AT & T, USA, August 11-August 20, 2010, visit paid by "FNU forskningsbevilling til diskret matematik".

*Wulff*, Claudia, University of Surrey, Guildford, UK, November 14-16, 2010.

### 2.5.2 Visiting Ph.D. students

*Bagheri*, Nasour, August 6-October 2, 2010

*Jeong*, Byeongseon, KAIST, May 28-July 1, 2010.

*Jang*, Sumi, KAIST, May 28-July 1, 2010.  
*Junge, Steffen*, Norwegian University of Science and Technology, Norway, February 1-June 30, 2010  
*Xiao*, Xiangchung, Xiamen University, China, January 1-April 26, 2010.

## 2.6 Administrative staff

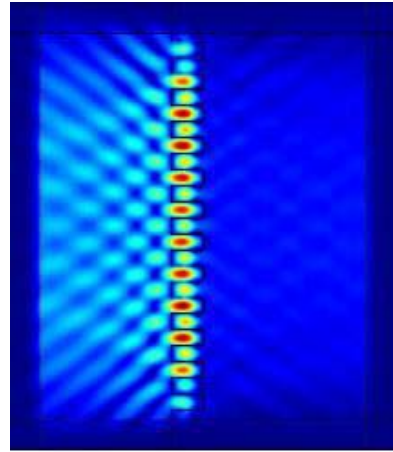
*Andersen*, Wanja, kontorfuldmægtig, (9 mths. from 1.4.10, overassistent 3 mths. to 31.3.10)  
*Haugland*, Kari, overassistent  
*Jensen*, Anna, kontorfuldmægtig  
*Louring*, Ulla, overassistent  
*Lundsgaard*, Dorte, korrespondent, kommunikationsmedarbejder, (11 mths. from 1.2.10)  
*Lægring*, Helle Vibeke, mag. art., administrati-onschef  
*Nielsen*, Ellen Juel, cand. silv., fuldmægtig, (2 mths. to 28.2.10)  
*Schmidt*, Karsten, cand. mag., project manager and teacher

## 2.7 Technical staff

*Madsen*, Poul-Erik, IT-funcion.

## 2.8. Emeriti

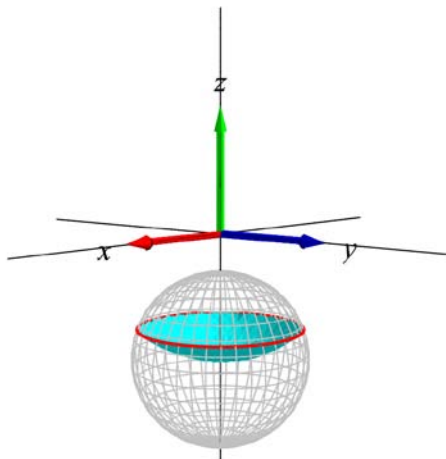
*Andersen*, Kurt Munk  
*Branner*, Bodil  
*Eising*, Jens  
*Jørsboe*, Ole  
*Hansen*, Vagn Lundsgaard  
*Karlsson*, Per W.  
*Kliem*, Wolfhard  
*Scheufens*, Ernst E.



## 3. Research

- European Study Group with Industry  
*Gravesen, Jens; Hjorth, Poul G.; Henriksen, Christian; Starke, Jens*

A Study Group is a forum where academic mathematicians work on problems directly related to industry. Workshops of this nature have taken place in Great Britain for a number of years, going back to 1963 when Prof. Alan Talyer started the Oxford Study Group with Industry. The coordination of Study Groups is now in the hands of European Consortium for Mathematics in Industry (ECMI), and the name is currently European Study Group with Industry (ESGI). At a meeting in 1997 of the ECMI Council it was decided that Study Groups should also be held outside Great Britain, and the first one of those was ESGI32 in Kgs. Lyngby, Denmark. The format of a Study Group is a week long meeting (Monday - Friday) where a number of companies on the first day of the meeting each present a research problem they believe to be of a mathematical nature. Each such problem is taken up by a group of mathematicians who, together with the company representative, work towards the solution of the problem, through Thursday afternoon. Friday is used to present in a plenary session the results from each of the problem groups. The reasons for the continuing success of the Study Groups are simple: The industrial participants get, for a very modest sum, a highly qualified 'think tank' of mathematicians to focus on their particular research problem. Besides a full or partial resolution of the problem, the companies establish useful contacts with international researchers. The academics benefit from new ideas and challenges from the real world, providing inspiration for both education and their own research. The success criterion for a Study Group is

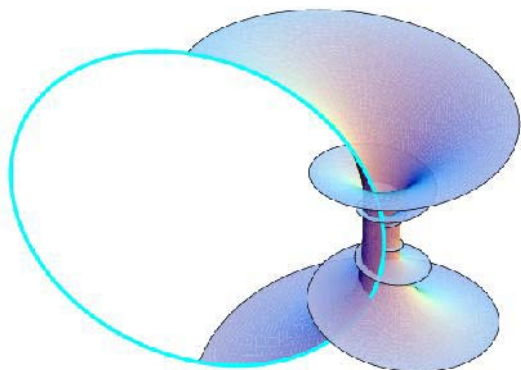


that participating companies experience the meeting as useful and that it brings them a significant step closer to the resolution of their problem. For the Danish study groups we also have the goal that it will establish closer ties between Danish Industry and Danish mathematicians. (In collaboration with University of Southern Denmark; Henrik Gordon Petersen, Morten Willatzen.)

- DCAMM Research School: International Researcher Education Activities

*Brøns, Morten*

The DCAMM International Graduate Research School is part of the activities of DCAMM, the Danish Center for Applied Mathematics and Mechanics. DCAMM is a framework for internationally oriented scientific collaboration between staff members at a number of departments at the Technical University of Denmark and Aalborg University. The Ph.D.-students of the School are members of DCAMM through the departments constituting DCAMM and they are enrolled in the relevant Ph.D.-programmes at DTU and AAU. The School's role is to provide for an interdisciplinary framework for education of young researchers in an international research environment. An important activity of DCAMM and the Research School are the DCAMM Symposia. These are bi-annual 3 day workshops with presentations mostly by Ph.D.-students and post.-docs. The School also maintains a programme of Ph.D.-courses / advanced schools. These courses (2.5 to 5 ETCS) are typically held as short intensive courses of 5 to 9 working days, enabling participation by students from all DCAMM institutions, foreign students as well as participants from industry. The governing body of the School is the Scientific Council of DCAMM.



### 3.1 Geometry

- Submanifolds associated to maps into loop groups.

*Brander, David*

Many special submanifolds (for example all "classical surfaces" such as constant mean curvature surfaces, constant Gauss curvature surfaces, Willmore surfaces etc) come in 1-parameter families, which leads to their representations as certain maps into loop groups. This results in methods for their construction, based on loop group factorizations. Such special submanifolds are sometimes called "integrable geometries". On the other hand, consideration of these loop group representations leads to natural generalizations of these submanifolds, and a framework for their systematic investigation. In this ongoing project, various aspects of this programme are studied, such as the identification of new integrable geometries, generalizing the known theory, and proving properties about the structure of loop groups in order to construct the special submanifolds.

- Generalizations of constant mean curvature surfaces via the loop group representation.

*Brander, David; Gravesen, Jens; Markvorsen, Steen*

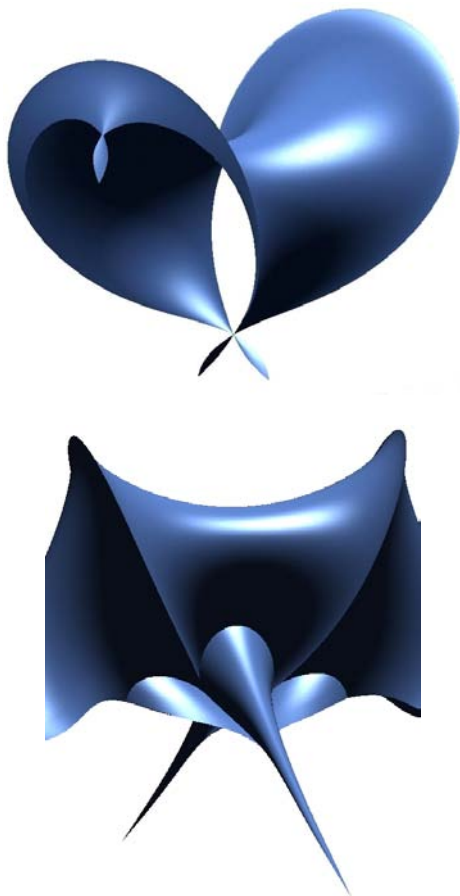
Viewed from the point of view of their loop group representation, constant mean curvature surfaces appear likely to be the first surfaces in a natural hierarchy of "integrable surfaces". This project aims to identify the other surfaces in this hierarchy.

- The geometric Cauchy problem for special surface via loop group methods.

*Brander, David*

Constant mean curvature (CMC) surfaces are mathematical models for the surface of a soap film, and other boundaries between different gasses/fluids. In principal, all CMC surfaces can be constructed from arbitrary holomorphic functions, using the method of Dorfmeister, Pedit and Wu (DPW). Little is known about the possibility to apply this method (and, more generally, loop group methods) to boundary value problems; that is, to find the holomorphic data necessary to construct a CMC surface with a prescribed boundary. The ability to do this would be of great interest in physical applications. This project began with this problem and is now expanded to include other types of surfaces. As a first step, we showed (2009) how to solve the Björling problem for nonminimal CMC surfaces, which is to construct the CMC surface which contains a given curve

and with tangent plane prescribed along this curve. In 2010 we solved the analogous problem for constant negative curvature surface, and also for timelike CMC surfaces. (Collaboration with J. Dorfmeister, TU Munich and Martin Svensson, USD).



Images: New examples of constant negative curvature surfaces obtained via our methods. These examples contain, respectively, a figure 8 curve and a cubic curve as geodesic principal curves.

- Singularities of integrable surfaces.

*Brander, David*

Integrable surfaces are surfaces which are solutions for integrable systems. They can be studied using loop group methods. Typical examples are surfaces of constant mean curvature or constant negative Gauss curvature. When the isometry group of the target space is not compact, the loop group decompositions used to construct the solutions is undefined at certain points. The behavior of the surfaces at such points has not been analyzed until now.

In recent (2008) work (joint with W. Rossman and N. Schmitt), it was shown, for the case of con-

stant mean curvature (CMC) surfaces in 2+1 dimensional space-time, that singularities of the surface arise at these “bad points” of the loop group. On the other hand, there has been a lot of interest recently in classifying generic singularities of analogous classes of surfaces, where almost every surface has singularities. In 2009 it has been shown that the loop group construction can be used to classify generic singularities of space-like CMC surfaces in 2+1 dimensional space-time. In 2010 (joint work with Martin Svensson) we obtained similar results for other classes of surfaces where a different kind of loop group splitting is used.



Images: The typical singularities of spacelike CMC surfaces in 2+1 dimensional Minkowski space, obtained via loop group methods. The first is a cuspidal crosscap and the second a swallow-tail singularity.

- Scroll Modelling

*Gravesen, Jens; Henriksen, Christian*

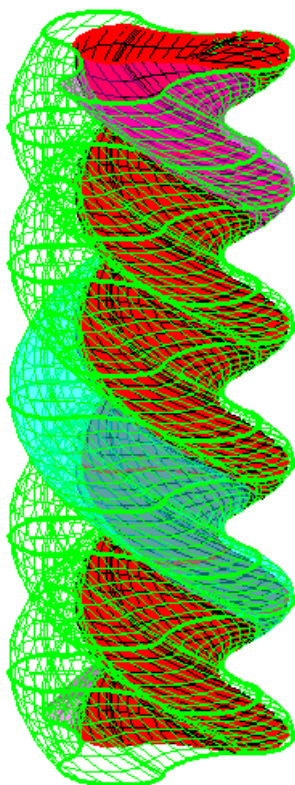
Scroll technology has since the seventies been widely used for air condition and efforts has been

made to use it for refrigeration and freezing. In Leon Creux original patent the main use was as a motor and recently this original idea has been taken up for the purpose of 'energy harvesting'. The idea is to use excess compressed air to produce electricity. In the project we want to combine geometric modelling done at DTU with dynamical modelling and physical experiments done in England. (In collaboration with Jihong Wang, University of Birmingham, England).

- Geometric effects in quantum structures

*Gravesen, Jens*

It is now possible to construct structures with thickness in nano-scale, so it can with good accuracy be considered as a surface. Eigen-energies and eigenstates of a quantum particle bound to such a nano structure depend on the geometry of the structure. Mathematically the question concerns the Helmholtz equation, i.e., eigenvalues and eigenfunctions for the Laplace operator, in a neighbourhood of the surface. We employ different techniques which with good accuracy reduce the problem from three to two dimensions. (In collaboration with Morten Willatzen, University of Southern Denmark.)



- Representing surfaces by the support function  
*Gravesen, Jens*

For a surface with non-vanishing Gaussian curvature, the Gauss map is regular and can locally be inverted. By specifying the support function as a function of the normal it is possible to construct the inverse Gauss map and the process is linear. Knowing the inverse Gauss map explicitly makes it easy to calculate geometric invariants such as the Gaussian and mean curvature and the principal curvatures and directions. Many important geometric constructions such as translation, rotation and offsets are easily expressed in terms of the support function. (In collaboration with Bert Jüttler, Johannes Kepler University, Linz, Austria, and Zbyněk Šír, Charles University in Prague, Czech Republic.)



- Faceting of surfaces

*Gravesen, Jens; Markvorsen, Steen*

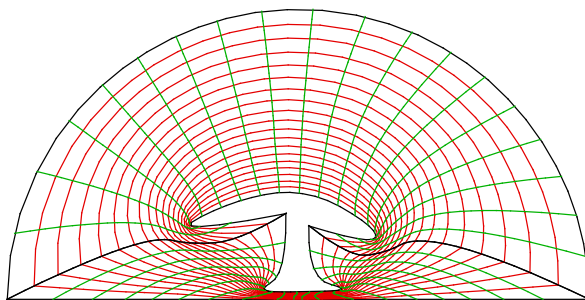
Faceting of surfaces is interesting from both engineering and an architectural point of view, as well as from a pure mathematical point of view. In this project we investigate ways of approximating a given smooth surface with a continuous surface consisting of planar facets. The facets are required to satisfy a number of constraints such as being quadrilaterals, having corners of valence three, having the same size, etc. It often happens that it is impossible to satisfy all constraints and then

approximate solutions must be sought for. (In collaboration with Henrik Almegaard and Anne Bagger, DTU Civil Engineering, Bert Jüttler, Johannes Kepler University, Linz, Austria, and Zbyněk Šír, Charles University in Prague, Czech Republic.)

- Isogeometric analysis-based shape optimization for maximizing magnetic energy

*Nguyen, Dang Manh; Evgrafov, Anton; Gravesen, Jens*

In 2007, a MIT group, led by Marin Soljagic, proposed a new method of transferring power wirelessly via strongly coupled magnetic resonators. The proposal provides possibilities for wirelessly recharging electrical devices such as laptops, cell phones. A couple of antennas were then proposed to improve efficiency of the transfer. For a given incident frequency, the shapes of the antennas play a decisive role of the transferring efficiency due to scattering effects, provided the distance between the antennas stays fixed. Therefore the problem requires a strongly accurate shape representing optimization method. In turn, isogeometric analysis (IGA) has recently been proven to fit well with shape optimization due to its ability to represent shapes exactly and the integration of geometry and analysis. To obtain the best possible solution, the shape is ideally allowed to vary freely. This gives rise to the problem of finding automated, robust and cheap methods to extend a given parametrization of the boundary to a volumetric one of the domain. It also requires robust methods to hinder shapes from being unphysical. With B-splines in hands, the issues can be handled effectively.



- History of Mathematics  
*Hansen, Vagn Lundsgaard*

Planning and editing a volume on "History of Mathematics" for the monumental "Encyclopedia of Life Support Systems" (EOLSS), which is published under the auspices of UNESCO. Also author of a few of the articles. EOLSS attempts to forge pathways between disciplines in order to show their interdependence and helps foster the transdisciplinary aspects of the relationship between nature and human society. It deals in detail with interdisciplinary subjects, but it is also disciplinary as each major core subject is covered in great depth, by world experts.

- Laplacian Processes on Submanifolds

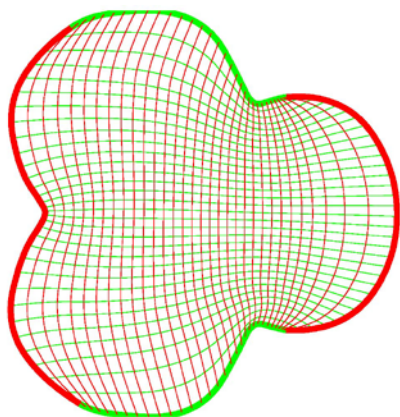
*Markvorsen, Steen*

The Laplacian controls a variety of very natural phenomena ranging from heat diffusion to volume growth. It is the purpose of this project to show precise bounds for specific values of measures such as the mean exit time for Brownian motion and isoperimetric inequalities for well chosen subsets of the submanifolds under consideration. The geometric structures under consideration are minimal (or close to minimal) submanifolds and minimal (or close to minimal) metric graphs. The bounds alluded to are obtained via comparison with corresponding values in constant curvature spaces and in other tailor-made warped product spaces. In collaboration with Vicente Palmer, Universitat Jaume I, Castellon, Spain.

- Minimal Metric Skeletons

*Markvorsen, Steen*

Metric graphs are considered as geometric background structures in their own right via an extension of the combinatorial Laplacian to the Friedrich extended Laplacian on the graphs which are considered as essentially one-dimensional submanifolds in the ambient space. The vertex minimality of these graphs guarantees not only self-adjointness of the Laplacian but also a direct comparison between functions in the ambient space and their restrictions to the graphs. This 'restriction comparison' is exploited in this project. Metric graphs may serve as good (Hausdorff-close) approximations to surfaces in 3-space. It is conjectured that minimal metric graphs (with straight line edges) in this sense can be used to approximate minimal surfaces modulo any given small number.



- Nonlinear p-Laplacian Comparison Theory

*Markvorsen, Steen*

We use drifted Brownian motion in tailor made warped product model spaces as comparison constructions to study p-hyperbolicity and p-parabolicity of a large class of submanifolds in ambient spaces with restricted curvature behaviour. It is expected that similar techniques will also give generalized isoperimetric inequalities as well as p-Laplace heat kernel estimates and mean exit time estimates for the corresponding nonlinear diffusion. In collaboration with Ilkka Holopainen, Helsinki University, Finland, and Vicente Palmer, Universitat Jaume I, Castellon, Spain.

- 3D Printing and 3D Scanning – Theory and Practice

*Markvorsen, Steen; Gravesen, Jens; Madsen, Poul-Erik*

This project is concerned with the theory and practice of 3D printing and 3D scanning. The project is concretely based upon a donation of a Z450 3D Printer and a Roland LPX 60 scanner from DTU's Strategic Fund. The purpose is twofold: To study and optimize 3D color printing and 3D scanning procedures on these platforms and to develop corresponding new assets for teaching, research, and prototyping in mathematics/geometry and applications. Part of the project is to interchange ideas concerning these topics with colleagues from DTU Mechanical Engineering, Informatics, Civil Engineering, and Chemistry. The findings and productions from this project will tentatively be integrated into the activities organized around Matematicum, the Mathematical Inspiratorium at DTU Mathematics, as well as into the relevant DTU courses e.g.: 01005 Mathematics 1, 01999 Geometric Operations in Plane and Space, 01234 Differential Geometry with Applications, and 02585 Computational Geometry Processing.

- Geometric Analysis: Classification Theory of Riemannian Submanifolds

*Markvorsen, Steen*

The general purpose of this project is to study the influence of curvature on the properties of solutions of certain partial differential equations whose leading symbol is the Laplacian or the p-Laplacian. One key instrument is the curvature controlled comparison of solutions in a given Riemannian (sub-)space with the corresponding solutions in a tailor made model space.

In collaboration with Vicente Palmer and Ana Hurtado, Universitat Jaume I, Castellon, Spain.

- Matematicum – The Mathematical Inspiratorium at DTU

*Markvorsen, Steen; Henriksen, Christian; Thomsen, Søren Steffen, Schmidt, Karsten; Starke, Jens; Hjorth, Poul G; Knudsen, Lars Ramkilde*

This project is concerned with the theme of unfolding mathematical concepts and results for students and other mathematically curious visitors to Matematicum via hands-on experiments and stories. Each story and activity is ideally centered around a well-defined mathematical crux, which is then to be uncovered, unfolded, and applied to properly understand a given, otherwise non-obvious – or maybe even mysterious – phenomenon. For example: How can two circular rotations combine to give the linear motion of a pump? What are the rotors actually doing in the Enigma encryption machine? Why and how does a (good) boomerang return? How do we make a swarm of intercommunicating robots collaborate to solve a given task? How do the ants find or construct their shortest pathways? Which roofs pick up the most solar energy throughout the year? Concerning content and development of concept: The Matematicum at the Department of Mathematics is a room which has been arranged to receive up to 15 visitors at a time. A boomerang 'story' and a robot swarming 'story' have been implemented and tested. A 3D printer and 3D scanner have been installed. The printer is in full operation and supplies concrete models of geometric shape and function such as minimal surfaces and ingenious pumps. A fume cupboard has been installed for proper and safe post-processing of the 3D-printed objects. An original three-rotor German military Enigma machine has been purchased. It is the essential central 'object' for great 'stories' and activities in the Matematicum concerning the history and development of modern cryptology. Matematicum was officially opened at a reception at DTU Mathematics on 6<sup>th</sup> March, 2008.

- Isogeometric analysis and shape optimization in fluid mechanics.

*Nielsen, Peter Nørtoft; Gravesen, Jens*

This project applies isogeometric analysis, a new computational methodology, to shape optimization problems within fluid mechanics. Isogeometric analysis unites the power to analyse complex engineering problems from finite element analysis (FEA) with the ability to represent complicated shapes smoothly from computer aided design (CAD). The method supports high degrees of continuity of the velocity and pressure fields in the analysis of the governing Navier-Stokes equations. The fixed form of the parametrisation of the flow domain allows the optimization procedure to change the shape freely without any need for heavy remeshing procedures. We apply the method to various concrete fluid shape design problems. The project is done in collaboration with Niels Leergaard Pedersen, DTU Mechanical Engineering.

- Optimal metrics on vector protein descriptors

*Røgen, Peter*

In this project an Euclidean metric on a protein descriptor vector space is optimized for combinations of the following objectives.

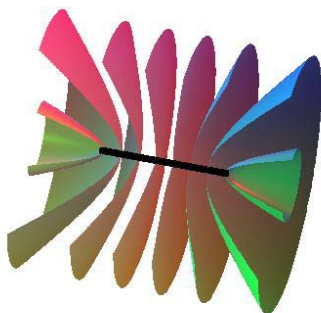
- 1) Maximal correlation with RMSD for similar protein pairs
- 2) Maximal separation of protein folds
- 3) Optimal automatic classification

It is examined how this best possible is done using linear semi definite optimization.

- Combined geometric and biochemical descriptors of proteins for fast automatic structural classification

*Røgen, Peter*

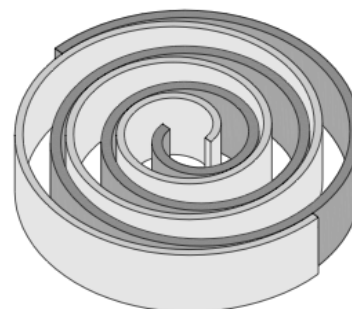
Using a coloring function along protein backbones that assigns secondary structure element types, purely geometric descriptors are extended to combine geometric and biochemical information. The aim is to obtain a fast automatic classification and protein structures.



- Sequence based local configuration space and knowledge based potential of proteins

*Røgen, Peter*

It is well known that proteins secondary structure may be predicted for about 80% of all sequence fragments and that at the order of 30% of all sequence fragments do not have structural preference. In this project the local structure of proteins is described continuously by length and distance excess. By cutting all 7-mer fragments from the known native protein structures, the configuration space and knowledge based potential of each 7-mer segment is approximated. The first test of these knowledge based potentials is to compare their ability to discriminate between decoy structures and the correct native fold to other methods. The longer term goal of this project is to make fold prediction. In collaboration with Patrice Koehl, Dept. of Comp. Sci. and Genome Center, UC Davis, USA.



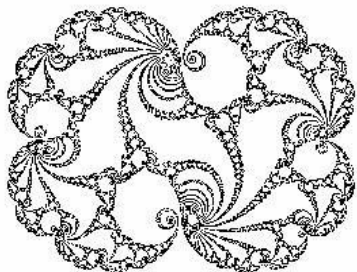
### 3.2 Dynamical systems

- Quasi-conformal surgery in holomorphic dynamics

*Branner, Bodil*

The technique of quasi-conformal surgery in holomorphic dynamics was initiated by Sullivan, Douady, Hubbard and Shishikura in the 1980'es. The method consists in forming new dynamical systems from given ones, by changing not only the dynamical plane (through cutting and sewing) and the mapping which defines the dynamical system, but also the complex structure in the new dynamical plane. The theory of quasi-conformal mappings is the basic tool. The surgery-technique is in particular successful when families of mappings can be related to each other in such a way that comparable dynamical properties are transferred to comparable structures in parameter spaces. In this joint project we will edit a graduate textbook under the above title. The first part of the book will contain basic material; the second part will consist of contributions by different authors who have all published important papers on sur-

gery. The first part of the book and the editing is done in collaboration with Núria Fagella, Universitat de Barcelona, Spain.



- Stabilization of vortices in the wake of a circular cylinder using harmonic forcing

Chamoun, George; Schilder, Frank; Brøns, Morten

We propose a very simple control mechanism to stabilize the Föppl vortices behind a circular cylinder. Fluid is blown in and sucked periodically into the cylinder at the fore and aft point. We show numerically that with sufficient amplitude this passive control may stop the vortices from moving away from the cylinder. However, the motion of the vortices may be chaotic.

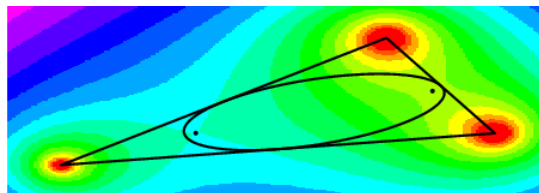


- Body/vortex interaction

Pedersen, Johan Rønby; Brøns, Morten

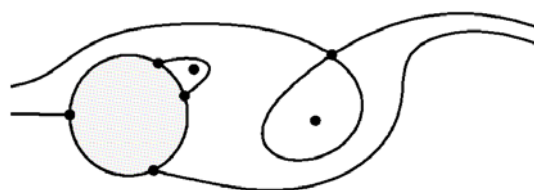
When a fluid flows around a body vortices are created. Understanding the motion of these vortices is of importance for predicting the forces on the body, and, if the body is not fixed, the motion of the body. In this project we study the interaction of the motion of a rigid body and a number of point vortices. We have obtained results on the transition from order to chaos in some simple systems with a few vortices. Also a study of the

“atmosphere” of a moving body, that is, vortices that may follow a translating and rotating body has been initiated. In collaboration with Hassan Aref, Niels Bohr visiting professor and Virginia Tech, DTU and Banavara Shashikant, New Mexico State University.



- Vortex topology in a magnetically driven flow  
*Brøns, Morten*

We consider the flow generated by sending a current through a thin layer of electrically conducting fluid. Below the fluid permanent magnets are oscillating harmonically and the interaction of the magnetic and electrical field gives rise to the creation of well-defined vortices. Based on the symmetry of the problem, we propose a bifurcation scenario for the flow pattern as time and system parameters vary. The scenario is confirmed by numerical computations. In collaboration with Eduardo Ramos, Sergio Cuevas and Alberto Beltrán, Universidad Nacional Autonoma de Mexico.

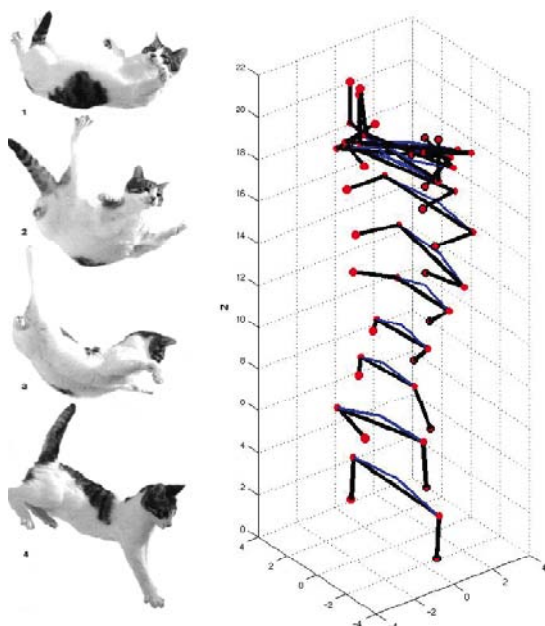


- Classification of meromorphic mappings  
*Henriksen, Christian*

A holomorphic dynamical system can be classified in several ways; for instance by analytical classes, quasi-conformal classes and topological classes. For rational mappings of the Riemann Sphere the quasi-conformal classes are completely understood up to the No Invariant Line Field Conjecture (due to Mañé-Sad-Sullivan and Sullivan-McMullen). However, for transcendental mappings, little is known of the quasi-conformal classes. The aim of this project is to remedy this situation, by understanding and describing the quasi-conformal classes of such mappings.

A transcendental function divides the plane into two sets: the Julia set, where the dynamics are chaotic, and the complement, the Fatou set, where the dynamics are tame. Meromorphic transcendental mappings differ from rational mappings in that they allow for infinitely dimensional deformation spaces. Related to this they can exhibit other types of Fatou domains, namely wandering domains, and Baker domains.

A first step for describing the quasi-conformal classes of entire transcendental functions is to understand the deformation space of an entire function on its Fatou set. The possible deformation spaces supported on Baker domains is as of now unexplored, except for work carried out by N. Fagella and C. Henriksen. A better understanding would complement work on classification of Baker domains done by Fagella and Baranski as well as Bergweiler. A second step is to understand the possibilities for deformations on the Julia set. Unlike what is conjectured to be true for rational maps, Eremenko and Lyubich have shown that an entire function can exhibit a Julia set of positive measure, which is not the whole plane, and yet supports an invariant line-field. In collaboration with N. Fagella, Universitat de Barcelona, Spain.



- Algorithms in holomorphic dynamics

*Henriksen, Christian*

Computers played an important role in reinvigorating the field of holomorphic dynamics in the eighties, and have played a part since then. Researchers have advanced the field by making numerical experiments and turning the observed

results into rigorous mathematics. However, the process also goes the other direction, with mathematics being turned into algorithms. One striking example of this is Thurston's Theorem. J.H. Hubbard and D. Schleicher constructed from the proof of this theorem the Spider Algorithm, that searches for a quadratic polynomial that realizes a certain prescribed combinatorics. J.H. Hubbard later generalized the Spider Algorithm to degree two rational maps. The aim of this project is first to document what is known, but never has been written down on the algorithms and then to generalize them so they work for rational maps of degrees exceeding two. In collaboration with S.L. Hruska, University of Wisconsin-Milwaukee.

- Road Structure Models

*Poul G. Hjorth*

Subject to small but repeated deformations from the passing vehicles asphalt roads slowly degrade until at some point they must be repaired or even replaced. Estimating the state of decay of a given road, such that preventive maintenance can be carried out in a timely fashion is a challenging problem. The state of decay must be measured in an accurate and repeatable fashion. The response of a particular segment of a road to the load from the wheel of a passing vehicle is an indicator of the state of the road, and can be measured from the vehicle by laser interferometry. This project (taking as point of departure a problem from the 51st European Study Group) aims creating a multi-parameter mathematical model of the road and of its response to the load a vehicle. Data from the Greenwood High Speed Deflectometer will be compared to the model.

- Crowd Dynamics.

*Hjorth, Poul G.; Starke, Jens, Corradi, Olivier*

We study dynamics of a 2-D crowd consisting of two populations of interacting pedestrians moving in opposite directions along a hallway and forced through an opening in a wall perpendicular to the hallway.

Several generic types of collective behavior are observed, among them a Hopf bifurcation leading to oscillations in pedestrian flux. We investigate the behavior of this phenomenon as system parameters and spatial boundary conditions are varied.

- Arctic Rossby Waves

*Hjorth, Poul G*

Due to the strong vertical stratification combined with its almost circular boundary, the Arctic Ocean supports internal centennial scale Rossby

modes. In this study we investigate these modes in a theoretical framework. We apply the free surface two layer model with a linear damping on the sphere and solve this in idealised geometries.

We solve this system numerically by a finite difference scheme based on the Arakawa C-grid.

We find that solutions to the system have a damping time scale comparable to the propagation time scale. Furthermore, this damping time scale is nearly independent of the local damping coefficient. For a circular geometry the amplitude is zero at the boundary.

Interestingly, for a more realistic sector-geometry we find finite amplitudes at the borders. We interpret this within the present model as anomalies in the halocline height being exported as fresh water anomalies via the Fram Strait where, further south, they may modulate deep water formation and the overall strength of the thermohaline circulation. In collaboration with Torben Schmith (Danish Meteorological Institute), and Mette Højgaard Pedersen.

### • Sequential Dynamical Systems

*Hjorth, Poul G.; Rani, Raffaele*

Sequential Dynamical Systems (SDS) model dynamical systems on graphs, but in contrast to, e.g. cellular automata, the vertex update does not take place globally, but follows a sequential rule. The dynamics of such discrete dynamical systems are completely encoded in their phase space: a directed graph whose edges and vertices represent all system configurations and dynamical transitions between them. Direct calculations and representations of the phase space is in most cases a computationally demanding task. For some classes of SDS one can, however, extract information about connected component structure of the phase space from the constituent elements of the SDS, such as base graph and vertex functions. Applications to biological networks, epidemics and social networks.

### • Continuation and Numerical Bifurcation Analysis in Experiments

*Schilder, Frank; Starke, Jens*

Experiments, simulation and continuation are three established methods for response analysis of physical systems or models thereof. All three approaches can be used for producing a bifurcation diagram of a specific system. However, each approach has distinctive advantages and disadvantages. While performing experiments is usually time- and resource intensive, it has the advantage that one investigates the actual system, which eliminates the possibility of modeling errors.

Performing simulations on a computer implementation of a model, on the other hand, is considerably cheaper and it is much easier to change model parameters than in experiments. However, brute-force computations for sophisticated models typically require substantial computational power. Furthermore, both methods share the drawback that they can only track stable responses, a restriction that is overcome by using continuation. While continuation can track stable as well as unstable responses, its application is most effective on carefully derived reduced models of relatively small dimension. A novel approach to overcome individual limitations of these methods is control based continuation, which aims at combining these methods in such a way that individual drawbacks are removed. In collaboration with Emil Bueero, Ilmar Santos and Jon Juel Thomsen, DTU Mechanics.

### • MATLAB Toolbox for Continuation

*Schilder, Frank*

Computing a covering (atlas) of implicitly defined manifolds is a key algorithm for computational bifurcation analysis. The goal of this development effort is the implementation of covering algorithms based on a novel formulation of the basic continuation problem. We are currently finalizing the core toolbox providing covering algorithms, event detection and data storage and retrieval. Ongoing and future projects are the implementation of problem-specific toolboxes, for example, for continuation in experiments. In collaboration with Harry Dankowicz, UIUC, USA.



*"Computation of Invariant Tori and Arnol'd Tongue Scenarios" During the ceremony on its opening day, the London Millennium Bridge showed a catastrophic synchronisation effect. Quote from*

*news.bbc.co.uk: “The bridge uses “lateral suspension” – an engineering innovation that allows suspension bridges to be built without tall supporting columns. The designers predicted it would be a “blade of light” across the Thames, “an absolute statement of our capabilities at the beginning of the 21st century.” Within days they closed it to be public.*

- Computation of Invariant Tori and Arnol'd Tongue Scenarios

*Schilder, Frank*

A famous phenomenon in synchronization problems leads to a two-parameter bifurcation diagram commonly referred to as the Arnol'd tongue scenario. One considers a system of coupled oscillators under the variation of two natural parameters, the coupling strength and a detuning parameter that controls the frequency ratio. The typical parameter plane of such a system has Arnol'd tongues with their tips on the decoupling line, opening up into the region where coupling is enabled, and in between these Arnol'd tongues, quasi-periodic arcs. These structures are related to the existence of quasi-periodic and phase-locked invariant tori. Since there routes exist to chaos involving the break-down of invariant tori, these phenomena attract considerable attention. A particular numerical complication arises from the fact that the invariance condition for phase-locked tori does not allow for a natural parametrization. As a consequence, existing methods are very limited and hardly applicable to real-world problems. The aim of this investigation is to develop a general purpose algorithm that is robust enough to be included in numerical bifurcation packages.

- Numerical Bifurcation Analysis of Symmetric (Hamiltonian) Systems

*Schilder, Frank*

Symmetry is a prominent feature in nature and science; many equations of physics honor certain symmetry groups. For example, Newton's equations of motion are invariant under Galilei transformations, reflecting the idea that physical laws should be independent of the current speed and position of an observer. An important feature of equations with symmetries is, that they may possess solutions with less symmetry than the equations themselves, that is, solutions with broken symmetry. Such solutions usually emerge from symmetric solutions via symmetry-breaking bifurcations. In this project we construct and study numerical methods for bifurcation analysis of systems with symmetries. In collaboration with Claudia Wulff, University of Surrey, UK.

- Equation-Free Analysis of Macroscopic Phenomena in Traffic Models

*Starke, Jens*

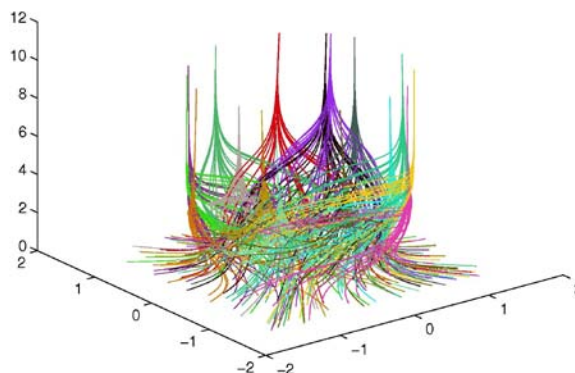
Equation-free approaches are used to investigate the macroscopic behavior of single lane traffic models. Even though the considered models are defined on a microscopic level, the quantities of interest live on a macroscopic level but quite often no explicit model equations are available for this. By short simulation bursts of the microscopic model it is possible to obtain sufficient information for a detailed numerical analysis of the macroscopic dynamics including continuation techniques and bifurcation analysis. The investigations focus on travelling waves of traffic jams such as the ratio of cars being involved in the traffic jam depending on model parameters like driver sensitivity or maximal velocity. This is a collaboration with R. Berkemer, AKAD Hochschule Stuttgart and A. Kawamoto and T. Shiga, Toyota CRDL, Japan.

- Analytical travelling wave solutions of traffic jam pattern formation on a ring for a class of optimal velocity traffic models

*Starke, Jens; Sørensen, Mads Peter*

A follow-the-leader model of traffic flow on a closed loop is considered in the framework of the extended optimal velocity model where a driver takes into account both the following car as well as the preceding car. Periodic wave train solutions which describe the formation of traffic congestion patterns were found analytically and their velocity and wave amplitudes were determined. This contains the standard forward-looking optimal velocity model as a special case. The analytical results are in very good agreement with the results of direct numerical simulation.

This is a collaboration with R. Berkemer, AKAD Hochschule Stuttgart, P. L. Christiansen, DTU, A. Kawamoto, Toyota CRDL, Japan and Y. Gaididei, Kiev, Ukraine.



- Processing of Sensory Information in the Olfactory System

*Starke, Jens*

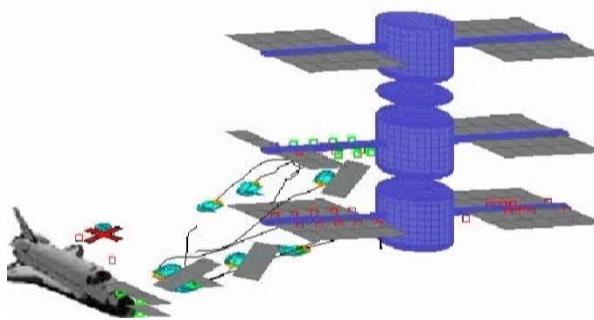
The olfactory system serves as important model case for other brain regions. It has a good experimental accessibility for several animals and relatively clear defined input and output. The odor signals are processed from receptor neurons over the glomeruli level to a neural network of mitral and granular cells while various types of nonlinear behaviour can be observed.

(1) Model of intracellular Ca oscillations due to negative feedback: A mathematical model for Ca oscillations in the cilia of olfactory sensory neurons was suggested. The underlying mechanism is based on direct negative regulation of cyclic nucleotide-gated channels by calcium/calmodulin and does not require any autocatalysis such as calcium-induced calcium release. Predictions of the model are in quantitative agreement with experiment, both with respect to oscillations and to fast adaptation. The influence of time dependent respiration cycles on the output dynamics is investigated. This is joint work with K. Nielsen, DTU, J. Reidl, University of Heidelberg, P. Borowski, Max Planck Institute for Physics of Complex Systems, A. Sensse, Frith Haber Institut, Berlin, M. Zapotocky, Max Planck Institute for Physics of Complex Systems and M. Eiswirth, Frith Haber Institut, Berlin.

(2) Modeling of axonal pathfinding in the olfactory system - sorting and convergence: Models with attracting and repulsive interactions were proposed which are able to reproduce the experimental findings of sorting and convergence during axonal pathfinding in the olfactory system. Many axon species, each represented by a huge number of axons, are spatially disordered at the beginning of their growth at the receptor neurons and converge by a self-organized process to a sorted state, i.e. axons of the same receptor type converge to a common position. Under certain model assumptions, it can be proved that the interacting many-particle system of different particle types converges to a sorted state. This is joint work with S. Kokkendorff, DTU, J. Strotmann, University of Hohenheim, N. Hummel, University of Heidelberg.

(3) Spatio-temporal dynamics in the olfactory bulb: Odors evoke a variety of stimulus specific spatio-temporal patterns on the levels of glomeruli and neural network of mitral and granular cells in the olfactory bulb which can be measured for mice in vivo using Ca and voltage sensitive dyes for optical imaging. A spatial independent component analysis (sICA) of this high-resolution imaging data was used to separate different neuronal populations based on their stimulus specific

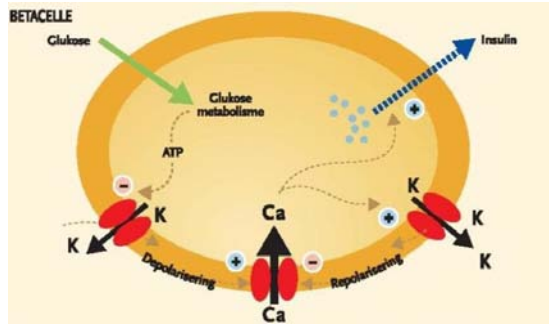
spatio-temporal activation. They can be identified as groups of glomeruli with different response latencies. Artifacts due to movement, heartbeat or respiration are automatically separated from the functional signal by sICA. Other applications were the somatosensory cortex of mice as well as the visual cortex of monkeys. Equation-free techniques allow for a systematic analysis of macroscopic network activities and their dependence on biological parameters such as kinetic parameters or network topology This is a collaboration with C. Ellsaesser, T. Kuner and J. Reidl, University of Heidelberg, J. Midtgaard, University of Copenhagen, D. Omer and A. Grinvald, Weizmann Institute of Science, and H. Spors, Max Planck Institute for medical research, Heidelberg.



- Control of distributed robotic systems by pattern formation principles

*Starke, Jens*

Time-dependent robot-target assignment problems with several autonomous robots and several targets are considered as model of flexible manufacturing systems. Each manufacturing target has to be served in a given time interval by one and only one robot and the total working costs have to be minimized (or total winnings maximized). A specifically constructed dynamical system approach (coupled selection equations) is used which guarantees feasibility of the assignment solutions. This type of control is based on pattern formation principles known in physics, chemistry and biology and results in fault resistant and robust behaviour. The performance of the suggested control is demonstrated and visualized with a computer simulation of autonomous space robots building a space station by distributed transporting several parts from a space shuttle to defined positions at the space station. This is a part-collaboration with C. Ellsaesser, University of Heidelberg, T. Fukuda, Nagoya University and M. Schanz, University of Stuttgart.



- Computation of superconducting wind turbine generators.

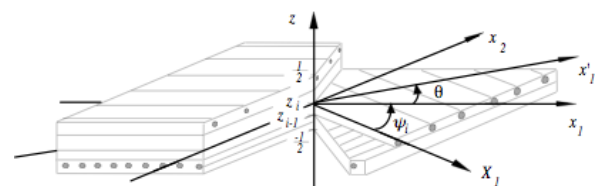
*Sørensen, Mads Peter; Zermeno, Victor Manuel Rodríguez*

The aim of this Ph.D. study is to build mathematical models of wind turbine generators with the traditional magnets replaced by superconducting coils fabricated of high temperature superconducting (HTS) materials. Commercially available HTS coated coils can deliver much higher magnetic fields than the strongest permanent magnets. This in turn can be used to design much lighter generators with direct drives without gearbox. The saving in weight may prove decisive for the constructing costs of future 10-20 MW wind turbines at sea, in contrast to the current maximum of about 3 MW generators.

We have set up nonlinear models for the induced magnetic field and its interaction with the HTS coils on a macroscopic level. The aim is to model a possible superconducting synchronous generator. Although superconducting synchronous machines have been successfully tested for several other power applications, no wind turbine has implemented this technology so far. One of the main issues to be considered is the fact that wind turbines are inherently subjected to dynamic power loads. Therefore, a generator of this kind will experience an AC ripple in the magnetic field with the changing wind speed. Consequently, AC losses are expected in the superconducting windings of the rotor. While this phenomenon can be reduced to some extent controlling the interaction with the electric grid and the blades angles, AC losses must be accounted for in the design of a superconducting wind turbine to ensure safety and performance during transient wind bursts. Therefore, we work on developing a fast and reliable tool to simulate the performance of electromagnetic devices with superconducting components and to provide a deeper insight into the feasibility of such turbines. One of the biggest issues regarding the simulation of superconductors is the substantial invested time to obtain realistic results.

This includes both the actual computing time and, more importantly, the time spent modeling every single application. Therefore, our aim has been to reduce both contributors to a minimum and make simulation of the electromagnetic properties of superconductors as easy and fast as possible.

In the last years, several approaches have been proposed to address this problem relying on the use of the finite element simulations. However, all PDE based formulations are still limited by the expensive computation of superconducting materials and the increased number of elements in the case of thin conductors such as the second generation superconducting wires that contain a micron thick superconducting layer. This problem is highly multiscale. (In collaboration with Niels Falsig Pedersen and Nenad Mijatovic DTU Electrical Engineering, Asger Bech Abrahamsen, Risø DTU, Philip Carne Kjær and Kenneth Krabbe, Vestas Wind Systems A/S, the Research School of DCAMM and the Superwind project consortium (<http://www.superwind.dk>).



- In silico models for blood coagulation.

*Sørensen, Mads Peter; Andersen, Nina Marianne*

In this industrial Ph.D.-project, together with the pharmaceutical company Novo Nordisk a/s, the aim is to develop a mathematical model of the blood coagulation cascade that can be used as a tool for improving the understanding of the coagulation processes and supporting the development of new haemostatic agents. The modelling includes solutions to reaction diffusion type equations with the added complexity of blood flow and activated surfaces. A model of the fully stirred reaction pathway has previously been established at Novo Nordisk and in the current project we have derived a model for in vitro coagulation and clot formation that include the spatial distribution of protein reactants and blood flow. This involves modelling with nonlinear partial differential equations (PDEs) and numerical solutions of these.

A mathematical criterion has been found for judging the validity of general models including diffusion, transport and interaction of biochemical species. The criterion guarantees non-



- Frames and their duals

*Christensen, Ole*

Frames are generalizations of bases, and allow complicated functions or signals to be expanded as linear combinations of elementary building blocks. They appear in several areas of engineering such as signal transmission, noise reduction, and time-frequency analysis. In order to apply the frame expansion, one needs to calculate or approximate one of the so-called dual frames. So far, most applications have dealt with a particular dual frame, the so-called canonical dual. Recently, it has been discovered that one can frequently find another dual frame, which is much more practical to work with. The goal of the project is to extend this result, and obtain convenient duals under various conditions

- FlowHead: Fluid Optimization Workflows for Highly Effective Automobile Development Processes

*Gregersen, Misha Marie; Gersborg, Allan Rou-lund; Sørensen, Mads Peter; Evgrafov, Anton*

FlowHead is aimed at strengthening the competitiveness of the European automotive industry by significantly reducing development time via integration of fluid optimization workflows into the product development process. The project is a collaborative effort between five European universities and six industrial companies, including two automobile manufacturers (Renault & Volkswagen). DTU is coordinating one of the work-packages in this project, dealing with topology optimization of flow domains. We try to advance the state-of-the-art techniques utilized for this purpose by the automobile industry, which are nowadays predominantly based on heuristic “optimality criteria”-type methods.

- Topology Optimization of Fluid-Structure Interaction Problems

*Evgrafov, Anton*

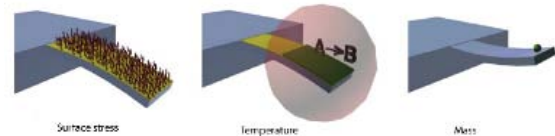
Together with Sebastian Kreissl, Kurt Maute and Georg Pingen from the University of Colorado, we develop a computational methodology for optimal design of transient fluid-structure interaction problems, where the structural part may undergo large elastic deformations as a result of the interaction with the fluid part or/and due to the application of external controls. On the road to achieve this end-goal, we have started with studying a simpler, time-independent, one-way coupled structure-fluid interaction, nevertheless incorporating the possibility of large elastic deformations of flow domains. The methodology has been applied to the problems of optimal design of multi-

functional elastic flow manifolds, which properties may be altered through large elastic deformations.

- NAMEC: Nano-mechanical sensors and actuators, fundamentals and new directions

*Marhadi, Kun; Sørensen, Mads Peter; Evgrafov, Anton*

As a part of a newly established VKR Centre of Excellence (a collaborative effort between the departments of Mathematics and Electrical Engineering at DTU and Pharmaceutical Faculty at Copenhagen University coordinated by the Department of Micro and Nanotechnology at DTU) we work on improving the sensitivity of nano-mechanical cantilever-based sensors. For example, for temperature sensors we would like to be able to detect temperature changes of only  $10^{-6}$ K. If such sensors were available, it would be possible to perform rapid and more accurate medical diagnostics and potentially even personalized medicines where medication is adjusted and released according to the need of patients. The latter is the longer term goal of this project.



- Inverse Boundary Value Problems

*Knudsen, Kim*

In inverse boundary value problems one considers questions regarding the unique determination, reconstruction and stability of a coefficient in a partial differential equation in a bounded domain from measurements of the solutions to the equation at the boundary of the domain. A particular example is the inverse conductivity problem, which is the mathematical background for the medical imaging technology known as Electrical Impedance Tomography. In this project we are in particular concerned with the theoretical and numerical study of a direct reconstruction method, the so-called D-bar method, for the inverse conductivity problem in two spatial dimensions. Moreover we consider problems, where the measurements are taken only on a part of the boundary. In collaboration with Matti Lassas, University of Helsinki, Finland, Jennifer Mueller, Colorado State University, USA, and Samuli Siltanen, Helsinki University, Finland.

- Direct numerical reconstruction of conductivities in three dimensions

*Knudsen, Kim*

The inverse conductivity problem is a non-linear severely ill-posed problem posed by A. Calderon in 1980. During the 1980's the three dimensional problem was in theory solved, but only recently computational aspects of the reconstruction algorithm has been considered. This project concerns the development of a stable numerical algorithm for the three-dimensional problem. The project is joint with Fabrice Delbarry and Per Christian Hansen at the department of Informatics and Mathematical Modelling at DTU and Jennifer Mueller, Colorado State University.

- Reconstruction of the sound speed from boundary data

*Knudsen, Kim*

This project deals with the numerical implementation of an algorithm due to Pestov-Uhlmann for the reconstruction of the sound speed in a two-dimensional medium from measurements of the so-called scattering relation at the boundary of the medium. In collaboration with Samuli Siltanen, Tampere University of Technology, Finland, and Gunther Uhlmann, University of Washington, Seattle, USA.



- MECOBS - The Research Network in Mathematical Biotechnology: Modelling, Estimation and Control of Biotechnological Systems.

*Pedersen, Michael*

Mathematical modelling and subsequent mathematical analysis has for decades been the common and firm ground for fruitful cooperation between the various technical sciences, the major breakthroughs in one field often being the impetus of research in the other. Being a relatively new field, biotechnology and systems biology has not yet had the need for very advanced mathematical modelling and analysis, but the rapid development of production techniques as well as more refined experimental methods calls for more elaborate mathematics than typically comprised in the biotechnological environments themselves. From a strict mathematical point of view, the areas of biotechnology and systems biology are, to a large

extent, using mathematical modelling and estimation based on both "imprecise definitions and inadequate methods". This is only a natural consequence of the fact that the fields have been driven so far by scientists with a background in chemistry and biology, but now the need for more advanced mathematical modelling and theory has become evident. This is in particular the case when the description of the systems in question is changed from a purely biological level to a description of the overall system dynamics and quantitative considerations. This also calls for the development of entirely new mathematical tools, leaving the hope that biotechnology and mathematics can develop the same synergy in the future that physics and mathematics has done for decades. By barrier-breaking workshops and knowledge-exchanging activities with the biotechnological and biological environments both nationally and internationally, the hope is to attract master- and Ph.D.-students to this interdisciplinary field and in this way establish a common ground for future research. The interdisciplinary nature of the subject is reflected in the theoretical background of the network members, and the initiative to cooperation with the scientific biotechnological environments at the universities and private companies is a major priority.

- Well-posedness of Partial Differential Equations

*Pedersen, Michael*

The Hilbert Uniqueness Method – HUM – invented by J.L.Lions is the most effective tool for theoretical studies of control mechanisms for Partial Differential Equations (PDEs). Based on advanced well-posedness results for the underlying PDEs, the method generates the most economical solution to the problem at hand. We will extend the well-posedness result so that the theory is applicable to also very non-smooth and nonlinear problems. In collaboration with E.Zuazua, Universidad Autonoma de Cantoblanco, Madrid.

- Control of Biological Systems:

*Pedersen, Michael*

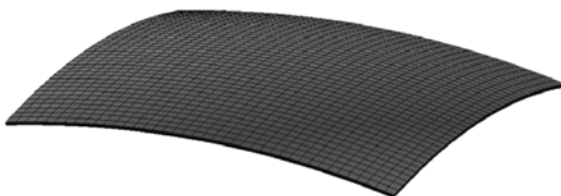
Together with researchers from Yangzhou University and the Technical University of Beijing we work on the control of ecological models (reaction-diffusion systems) . Due to major pollution problems caused by intensive migration to the cities, this research has very high priority in China. We will apply HUM to the coupled systems and in this way propose control mechanisms that are optimal for the underlying linear models. Then we will combine the results with recent existence

and uniqueness results and in this way propose a non-linear HUM method for such ecological models. In collaboration with L.Zhigui, Z.Lin, Yangzhou University, PRP China.

- Control of reaction-diffusion systems occurring in biotechnology and system biology.

*Pedersen, Michael*

Reaction-diffusion partial differential equation (PDE) models occur frequently in many applications; recently complicated non-linear models have been introduced to model e.g. living cells interacting with the environment or to model the metabolism of the single cell. Up to now, the typical approach to modelling these phenomena has been to consider a system of ordinary differential equations and subsequently estimate the parameters of these in order to produce predictive models. The idea in this project is to model the cellular response of e.g. yeast to hyperosmotic shock by integrating the full thermodynamic pde-description of the volume regulation and the osmotic pressure with the biochemical reaction network comprising receptor stimulation, cascade dynamics and activation of gene expressions. The full pde model will make it possible to take into consideration the spatial heterogeneity of the cells and the outcome of this project should hopefully be a computer simulation programme that could be the starting point in the modelling and analysis of cellular signaling in other living cells. At least two important related issues here are the questions of coexistence (the possibility of simultaneous existence of e.g. two species) and control: can we design a system where one of the species controls the other. The possible control mechanisms are of a highly complicated nature and usual finite-dimensional approximation techniques fail due to the fact that the approximation must be performed in rather delicate function spaces. The idea is here to apply the PDE-control mechanism HUM (Hilbert Uniqueness Method) proposed by J.L.Lions, which has recently been adapted to nonlinear situations, to this particular setting. If successfully applied, HUM will immediately describe a both optimal and robust algorithm for the solution of the control problem. In collaboration with Institute of Biomathematics and Biostatistics, Munich.



- Boundary Control of Plates.

*Pedersen, Michael*

Applying a new functional analytical method we have extended the classical HUM framework to a large class of hyperbolic PDE-models. The method is based on ideas from pseudo differential operator theory and reveals how HUM is an advanced, infinite dimensional formulation of well-known finite dimensional control theory. We have successfully applied this program to the Mindlin–Timoshenko plate system, and the idea is now to investigate possible numerical implementations of the method. This is far from trivial, since even in the 1-d case for the classical wave equation, the natural discretization is very problematic. Collaboration with the group of E.Zuazua, Universidad Autonoma de Cantoblanco, Madrid.

- Multi-material design optimization of composite structures

*Stolpe, Mathias; Munoz, Eduardo*

The use of composite materials has been steadily growing in industry in recent years. A major challenge in the field of optimal design of composite structures is to develop models and optimization methods which use rational design of the local material properties to meet specific design criteria, while still being solvable for large scale problems. In this project we develop new such models and optimization methods for optimum design of multi-material composite structures, e.g. structures which are made of glass or carbon fiber reinforced polymers as well as sandwich core materials. The models take design criteria on the global structural stiffness and local strength to avoid failure of the composite structure into account. In collaboration with Professor Erik Lund, Institute of Mechanical Engineering, Aalborg University.

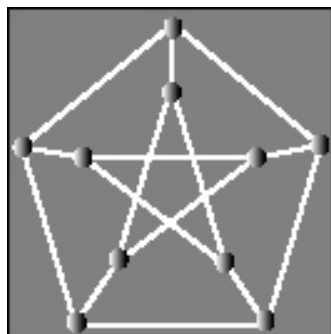
- Dynamical behavior of mathematical models for structured systems.

*Zhang, Lai; Knudsen, Kim*

This Ph.D. study concerns the dynamics of ecological communities. We aim to investigate the interactions of coexisting populations of trait-based species from both ecological and evolutionary points of view. The study can advance our understanding on how a food web is developed and what are the main constraints on the species richness complexity and stability.

The work is composed of two parts. First, theoretical models including species interactions, characteristics, and interference competition are developed through metabolic theory; spectrum theory and adaptive theory and so on. Secondly, by means of analytic analysis and numerical simula-

tions, reconciliation of species spectrum and food web representations of a community, interference induced speciation in size structured population model, cannibalism induced bistability in size structured population model, stability of community spectrum, and evolutionary steady states of food webs from evolution and immigration are examined. The works are co-supervised by Ken Haste Andersen, (DTU Aqua) and Uffe Thygesen, Høgsbro (DTU Aqua).



### 3.4 Discrete Mathematics

- Mathematical coding theory  
*Beelen, Peter; Høholdt, Tom*

Error-correcting codes are used to obtain reliable and fast transmission of information in a modern digital communication system. When data are transmitted they can be corrupted by “noise” so the received symbols are not all the same as the sent ones. This is the case in satellite communication, mobile communication and data storage. Error-correcting codes are used in the following way: suppose A wants to transmit information to B. A creates a *codeword* by adding extra symbols to the information (this is called encoding) and sends it to B. What B receives is a corrupted version but by (cleverly) using the extra symbols it is possible to recreate the codeword, at least with high probability (this process is called decoding). The problem now is to construct codes that can correct as many errors using as few extra symbols as possible and also, such that the en- and decoding algorithms have low complexity. Many of the mathematical problems that arise in connection with the construction and usage of error-correcting codes can be treated using algebraic, geometric and combinatorial methods. These questions have a technical origin but lead to many interesting and hard mathematical problems. It is these fundamental mathematical problems that the current project addresses. Some of the issues in detail are:

Codes on graphs: There is a growing interest in graph theoretical descriptions of error-correcting codes as a way to get codes with lower decoding complexity. Most of the known results are asymptotical and not too convincing for real applications. We are investigating specific constructions, in particular constructions that use earlier results on concatenated codes and codes based on finite geometries.

Decoding of Reed-Solomon codes and concatenated codes: Recent decoding methods for Reed-Solomon codes makes it possible to correct errors beyond half the minimum distance. We investigate the limitations of these new methods also in order to gain a deeper understanding of the distance properties of the codes.

Algebraic geometry codes: Algebraic geometry codes are constructed by evaluating functions from a suitable vector-space over a finite field in points on an algebraic variety. For example the group recently studied codes coming from affine parts of Grassmann varieties. Using algebraic curves it has been possible in this way to construct codes that are “better” than previously known codes. The main problems are explicit constructions both of the varieties and the vector-spaces as well as getting efficient decoders.

In the past year, the group has found decoders for some classes of algebraic-geometry codes that are more efficiently than previously known ones.

Codes and Boolean functions: Boolean functions with cryptographically strong properties can be constructed by finding supercodes of a first order Reed-Muller code. Such a supercode is then required to have as high a minimum distance as possible. Reed-Muller codes are basic examples of algebraic geometry codes, so algebraic techniques can be used to construct and investigate such supercodes. The research on Boolean functions is being carried out in cooperation with the cryptography group.

- Analysis of SHA-3 hash function / Formal analysis of cryptographic hash functions. (August 2009 - July 2011)

*Praveen Gauravaram*

Cryptographic hash functions are one of the most important tools used in the design of efficient cryptographic protocols such as digital signatures that enable secure communications over the Internet. Cryptographic protocols are often proved secure assuming that the underlying hash functions are secure. Ever since the hash function SHA-1 has been adopted as the Federal Information Processing Standard (FIPS) by the NIST, U.S, it has been deployed in many provably secure cryptographic protocols.

Security vulnerabilities that are exposed in SHA-1 and other standard hash functions have dramatically reduced our confidence in using current hash functions as secure mechanisms in the cryptographic protocols. In search of a secure hash function, NIST, U.S., initiated a global competition in 2007 to select a new hash function by 2012 which will be referred to as SHA-3. Many popular hash function constructions and those submitted to the SHA-3 competition are based on block ciphers.

The goal of this research project is to carry out formal as well as concrete analysis of hash functions based on block ciphers thereby contributing to the understanding of the theory of hash functions and selection of SHA-3. This analysis will strengthen our confidence in proving the security of cryptographic protocols and later implement them using hash functions whose security is known. This project has been jointly sponsored by FTP and FNU.

- Highly Nonlinear Functions

*Leander, Gregor*

While a lot of progress has been made in the last decades in the area of symmetric cryptography there are still many fundamental problems that could not be solved yet. These questions are of theoretical interest but also have direct impact on the practical design of stream and block ciphers.

Many attacks on symmetric ciphers are based on observations on the Boolean functions describing the system. The formalization of known attacks, most notably the differential and linear cryptanalysis and more recently the algebraic attacks, have led to design criteria related to these Boolean functions. However for most of these criteria it is unclear how to construct functions that meet these criteria the best way possible, moreover even the optimal values for some classical criteria as the nonlinearity and the resistance against differential cryptanalysis are unknown.

This project aims at finding Boolean functions with an optimal resistance against known attacks. The approach hereby is twofold: On the one hand advanced computer algorithms are developed to find optimal functions within the huge space of Boolean functions. On the other hand better bounds and general constructions are derived using results related to coding theory.

- Central digraphs.

*Leander, Gregor and Thomassen, Carsten*

This project is a collaboration between André Kündgen, Associate Professor, California State University San Marcos, and Lektor Gregor Leander and Professor Carsten Thomassen, DTU.

A directed graph is called *central* if the square of its adjacency matrix has a 1 in each entry. Central digraphs are directed analogues of the so-called friendship graphs. Today, central digraphs are of interest in cryptography. For example, the bit permutation used in the block cipher PRESENT gives rise to a central digraph with 16 vertices.

It has been conjectured that every central directed graph can be obtained from a standard example by a sequence of simple operations called *switchings*, and also that it can be obtained from a smaller one by an extension. We disprove these conjectures and present a general extension result which, in particular, shows that each counterexample extends to an infinite family.

- Analysis and design of encryption systems in constrained environments

*Knudsen, Lars R; Zenner, Erik*

One defining trend of this century's IT landscape will be the extensive deployment of tiny computing devices. Not only will these devices feature routinely in consumer items, but they will form an integral part of a pervasive and unseen communication infrastructure. Security and privacy threats against this technology have to be mitigated by the use of cryptographic solutions. However, the current state of the art is often too cumbersome to be used in such resource-restrained environments. Thus, the aim of this project is to develop lightweight cryptographic systems, such as special-purpose encryption algorithms and protocols, and to analyze existing proposals. In all cases, the right trade-off point between security and compact hardware design has to be found. Collaboration with Horst-Görtz-Institute for IT-Security, Ruhr-University Bochum, Germany and France Telecom R&D, Issy les Moulineaux, France.

- Analysis and design of hash functions

*Knudsen, Lars R.*

A cryptographic hash function is a function which takes a binary string of arbitrary length and which outputs a binary string of a fixed, predetermined length. For use in cryptology it must be "hard" (impossible in practice) to find two different inputs yielding the same output through the hash function. We have devised two new constructions for hash function designs. In collaboration with the Institute for Applied Information Processing and Communications at Graz University of Technology, Austria. One proposal, called Grøstl, was submitted as a candidate for a new US governmental standard for cryptographic hashing in a world-wide open competition. The winner of the competition is expected to be announced in 2012.

In the next few years this project will consist of trying to cryptanalyse other submissions to this competition.

- Analysis of symmetric-key ciphers by means of numerical methods

*Knudsen, Lars R.*

This project concerns cryptanalysis of symmetric-key cipher by means of numerical methods. Such methods are normally applied to systems of real numbers, whereas symmetric-key primitives are defined on Boolean values, that is, numbers which take only the values 0 and 1. A conversion from Boolean numbers to real numbers is far from trivial, but preliminary analysis has demonstrated that this idea has some potential. This project is supported by the The Danish Council for Technology and Innovation.

- Post-quantum cryptography

*Knudsen, Lars R.*

In general there are only very few known methods for doing so-called public-key cryptography today. Public-key cryptosystems are an integral part of the infrastructures of our information network society today, in particular they are the basis of digital signatures and crucial for security in communication, for example in electronic commerce. If the methods we use should turn out to be less secure than expected, we will be in trouble since it is unclear what the alternatives should be. The development in public-key cryptanalysis has been dramatic in later years and it has been necessary to upgrade many existing systems to accommodate for new cryptanalytic approaches. This general worry about the security of existing systems has become much more concrete in connection with research on so-called quantum computers. A quantum computer works fundamentally differently from the classical computer, and certain problems can be solved considerably faster on quantum computers than on the computers we use today. As an example, it has been shown that the security of all public-key cryptosystems that are in use today can be broken using a quantum computer, and (almost) all other cryptosystems will have a much lower security level in the presence of a quantum computer than they have today. That is, if it is possible to build *sufficiently large* quantum computers. The latter is a tremendous technical challenge, and quantum computers today can only work with at most about 10 bits. But one must expect that this development will go on and that quantum computers with considerable computing power will be a reality in a foreseeable future.

Therefore it is important already now to start the process of finding new paradigms on which we can build the cryptographic systems for the future.

- Analysis and design of stream ciphers

*Knudsen, Lars R. and Zenner, Erik*

Stream ciphers are encryption algorithms for applications with special performance or resource requirements. Since they are optimized to provide as much throughput or to require as little hardware as possible, their security margin is much lower than that of other encryption techniques. Thus, designing stream ciphers requires a high degree of cryptographic understanding, and many fielded designs have been broken in the past.

- Graphs on higher surfaces

*Thomassen, Carsten*

This project is a collaboration between Dr. Kenichi Kawarabayashi, National Institute of Informatics, National Center of Science, Japan, and Professor Carsten Thomassen, DTU, concerning extendibility of results on planar graphs to higher surfaces. The project is supported (in the form of travel expenses) by FNU (Rammebevilling i Diskret Matematik) and National Center of Science, Tokyo, Japan.

- Chromatic numbers and graph decomposition.

*Thomassen, Carsten*

In 2005 the Marie Curie Fellow Janos Barat and his supervisor Carsten Thomassen made the conjecture that, for every tree  $T$ , it is possible to decompose a graph of sufficiently large edge-connectivity into copies of  $T$ . Although we could not at the time verify this for any single non-trivial instance of  $T$ , we showed that, when  $T$  is the claw, the conjecture is intimately related to Tutte's 3-flow conjecture, motivated by the classical 3-color theorem of Grotzsch.

In 2010 Carsten Thomassen obtained a breakthrough, namely a proof of the so-called weak 3-flow conjecture posed in 1988 by F.Jaeger. Among the applications, the decomposition conjecture is now verified for each star.

- Quadrangulations in triangulations on surfaces.

*Thomassen, Carsten*

This project is a collaboration between André Kündgen, Associate Professor, California State University, San Marcos, and Professor Carsten Thomassen, DTU, concerning spanning quadrangulations.

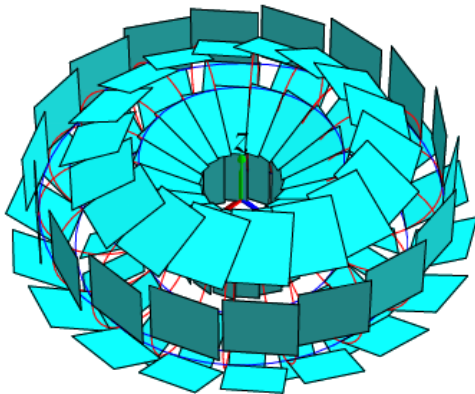
gulations in triangulations. The research is motivated by the conjecture of Kundgen that every triangulation with large width has vertex-2-coloring without any monochromatic triangle. This problem can be reformulated in terms of spanning quadrangulations. We use alternating cycles to shed light on this problem.

- Software Side-Channel Attacks

*Zenner, Erik*

Traditionally, the security of cryptographic systems is considered in an ideal environment, where the adversary can not access the computer that does the cryptographic work. However, a real-world attacker will often use malware (virus, Trojan horse etc.) on the user's PC to collect information about the cryptographic operations and keys. This type of attack is called a software side-channel attack.

Within this research focus, we try to mitigate some attacks of this type. One class of attacks called "cache timing attacks" can be prevented by appropriate implementations, but also by clever design of the cryptographic algorithms. A much broader class of attacks can be countered by the so-called white-box cryptography: A pseudo-random mixing of the key and algorithm that makes it hard for a malicious program to find out what is actually going on on the computer. While it can be proven that no perfect solution to this problem exists, it seems that protection against a limited attack tool like a virus can be achieved.



### 3.5 Ph.D. projects

- Dimension reduction methods applied to mechanical systems.

15.12.09 to 14.12.12.

*Michael Elmegård*

Supervisors: *Jens Starke; Jon Juel Thomsen, Anton Evgrafov*

- List decoding of folded Reed-Solomon codes - and algebraic geometry codes.

*Johan S. Rosenkilde Nielsen*

Supervisors: *Peter Beelen; Tom Høholdt.*

- Modelling and simulation of road structures.

*Louis Pedersen*

Supervisors: *Poul G. Hjorth; Kim Knudsen.*

- Modelling, Simulation and Optimization of Object-Gripping by Robots

*Marie Bro Dunn*

Supervisor: *Poul G. Hjorth.*

- Iso-geometric analysis and shape optimization in electromagnetism

From 15.02.09 to 14.02.12

*Dang Manh Nguyen*

Supervisors: *Jens Gravesen; Anton Evgrafov.*

- Iso-geometric analysis and shape optimization in fluid mechanics

From 01.02.09 to 31.01.12

*Peter Nørtoft Nielsen*

Supervisors: *Jens Gravesen; Niels Leergaard Pedersen.*

- Multi-material design optimization of composite structures

*Eduardo Munoz*

Supervisor: *Mathias Stolpe*

- Topology Optimization for Crashworthiness Design Using Approximate Procedures

*Oded Amir*

Supervisors: *Mathias Stolpe; Ole Sigmund.*

- Topology Optimization Problems with Design-Dependent Sets of Constraints

*Marie-Louise Rasmussen*

Supervisors: *Mathias Stolpe; Anton Evgrafov; Ole Sigmund.*

- Cryptanalysis of Symmetric Cryptosystems by means of Numerical Methods

*Julia Borghoff*

Supervisor: *Lars Ramkilde Knudsen.*

- Post-quantum cryptology

*Valérie Gauthier Umana*

Supervisors: *Lars Ramkilde Knudsen; Gregor Leander.*

- In silico models of blood coagulation

*Nina Marianne Andersen*

Supervisors: *Mads Peter Sørensen; Sten Hvass Ingwersen; Ole Hvilsted Olsen.*

- Computation of superconducting wind turbine generators.

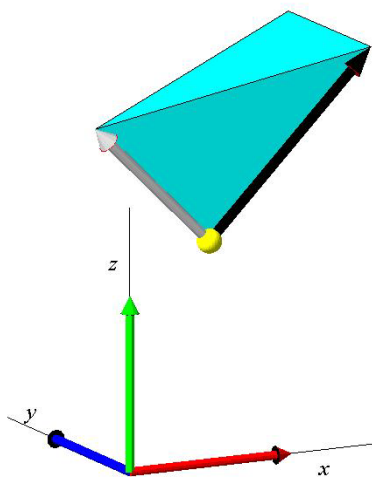
*Victor Manuel Rodríguez Zermeno*

Supervisors: *Mads Peter Sørensen*; Niels Falsig Pedersen; Ramasamy Anbarasu, Vestas Technology R&D.

- Dynamical behavior of mathematical models for structured ecosystems

*Lai Zhang*

Supervisors: *Kim Knudsen*; Ken Haste Andersen; Uffe Høgsbro Thygesen.



### 3.6. E-learning

- "E-learning project HEROS for first year math - new ways of learning"

*Markvorsen, Steen; Schmidt Karsten*

The aim of this project is to develop a new web based learning platform for the course Engineering Mathematics 1 – a platform which combines cutting edge e-learning materials and strategies with lectures, textbooks, weekly menus, and Maple demos. The main task is to further support the multifaceted architecture of the course while still keeping it clear-cut and transparent. The idea is to make room within this architecture for several interlinked teaching styles and teaching materials and thus enhance the possibility for the individual student to find and operate his or her own most effective learning style. New "nonlinear" learning objects including text files, animations, video clips etc. will be developed and packed in order to create multiple entries into the process of understanding the key mathematical concepts. The project is conducted in collaboration with Søren

Enemark (student at DTU) and Kasper Skårhøj (Consultant at LearningLab DTU) and continues an earlier project initiated with Helle Rootzén, DTU Informatics now with Karsten Schmidt as project manager.



## 4. Research publications

### 4.1 Articles in Journals, peer reviewed

Alstrøm, Tommy Sonne; Sørensen, Mads Peter; Pedersen, Niels Falsig; Madsen, Søren  
**Magnetic Flux Lines in Complex Geometry Type-II Superconductors Studied by the Time Dependent Ginzburg-Landau Equation.**  
 In: Acta Applicandae Mathematicae, pp. 1-12 (2010). Springer Netherlands.

Amir, Oded; Stolpe, Mathias; Sigmund, Ole  
**Efficient use of iterative solvers in nested topology optimization**  
 In: Structural and Multidisciplinary Optimization, vol.: 42(1), pp. 55-72 (2010). Springer.

Andersen, Nina Marianne; Sørensen, Mads Peter; Efendiev, Messoud A.; Olsen, Ole Hvilsted; Ingwersen, Steen H.  
**Modelling of the Blood Coagulation Cascade in an In Vitro Flow System.**  
 In: International Journal of Biomathematics and Biostatistics, vol.: 1(1), Article no. 1, pp. 1-7 (2010).

Bagheri, Nasour; Gauravaram, Praveen; Naderi, Majid; Sadeghiyan, Babak  
**EPC: A Provably Secure Permutation Based Compression Function**  
 In: I E I C E Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.: E93-A(10), pp. 1833-1836 (2010). Denshi Jouhou Tsuushin Gakkai.

Bartuccelli, Michele; Deane, Jonathan H.B.; Gentile, Guido; Schilder, Frank  
**Arnol'd tongues for a resonant injection-locked frequency divider: analytical and numerical results**

In: *Nonlinear Analysis: Real World Applications*, vol.: 11(5), pp. 3344-3362 (2010). Elsevier Ltd.

Beelen, Peter; Brander, Kristian

**Efficient list decoding of a class of algebraic-geometry codes**

In: *Advances in Mathematics of Communication*, vol.: 4(4), pp. 485-518 (2010). American Institute of Mathematical Sciences.

Beelen, Peter; Brander, Kristian

**Key-equations for list decoding of Reed-Solomon codes and how to solve them**

In: *Journal of Symbolic Computation*, vol.: 45(7), pp. 773-786 (2010). Academic Press.

Beelen, Peter; Bassa, Alp

**The Hassa-Witt invariant in some towers of function fields over finite fields**

In: *Sociedade Brasileira de Matematica. Boletim, Nova Serie*, vol.: 41(4), pp. 567-582 (2010). Springer.

**Bifurcation analysis in a vortex flow generated by an oscillatory magnetic obstacle**

In: *Physical Review E (Statistical, Nonlinear, and Soft Matter Physics)*, vol.: 81(3), Article no. 036309 (2010). American Physical Society.

Bogomolny, Michael

**Topology optimization for free vibrations using combined approximations**

In: *International Journal for Numerical Methods in Engineering*, vol.: 82(5), pp. 617-636 (2010). John Wiley & Sons Ltd.

Brander, David

**Singularities of spacelike constant mean curvature surfaces in Lorentz-Minkowski space**

In: *Mathematical Proceedings of the Cambridge Philosophical Society* (2010).

Brander, David; Dorfmeister, Josef

**The Björling problem for non-minimal constant mean curvature surfaces.**

In: *Communications in Analysis and Geometry* (2010).

Brander, David; Rossman, Wayne; Schmitt, Nicholas

**Holomorphic representation of constant mean curvature surfaces in Minkowski space: Consequences of non-compactness in loop group methods**

In: *Advances in Mathematics*, vol.: 223(3), pp. 949-986 (2010). Academic Press.

Branner, Bodil; Dias, Kealey

**Classification of complex polynomial vector fields in one complex variable**

In: *Journal of Difference Equations and Applications*, vol.: 16(5-6), pp. 463-517 (2010). Taylor & Francis Ltd.

Brøns, Morten; Kaasen, Rune

**Canards and mixed-mode oscillations in a forest pest model**

In: *Theoretical Population Biology*, vol.: 77(4), pp. 238-242 (2010). Academic Press.

Brøns, Morten; Bisgaard, Anders Villefrance

**Topology of vortex creation in the cylinder wake**

In: *Theoretical and Computational Fluid Dynamics*, vol.: 24(1-4), pp. 299-303 (2010). Springer.

**Christensen, Ole; Kim, H. O.; Rae Young, Kim Gabor windows supported on [-1,1] and compactly supported dual windows**

In: *Applied and Computational Harmonic Analysis*, vol.: 28(1), pp. 89-103 (2010). Academic Press.

Christensen, Ole; Rae Young, Kim

**On Dual Gabor Frame Pairs Generated by Polynomials**

In: *Journal of Fourier Analysis and Applications*, vol.: 16(1), pp. 1-16 (2010). Birkhäuser Boston.

Christensen, Ole; Goh, Say Song

**Pairs of oblique duals in spaces of periodic functions**

In: *Advances in Computational Mathematics*, vol.: 32(3), pp. 353-379 (2010). Springer New York LLC.

Gauravaram, Praveen; Kelsey, John; Knudsen, Lars Ramkilde; Thomsen, Søren Steffen

**On hash functions using checksums**

In: *International Journal of Information Security*, vol.: 9(2), pp. 137-151 (2010). Springer.

Høholdt, Tom; Beelen, Peter; Ghorpade, Sudhir Ramakant

**Affine Grassmann codes**

In: *IEEE Transactions on Information Theory*, vol.: 56(7), pp. 3166-3176 (2010). IEEE.

Karamehmedovic, Mirza; Sørensen, Mads Peter; Hansen, Poul Erik; Lavrinenko, Andrei

**Application of the method of auxiliary sources to a defect-detection inverse problem of optical diffraction microscopy**

In: *European Optical Society. Journal. Rapid*

Publications, vol.: 5, p. 10021 (2010). European Optical Society.

Knudsen, Kim

**Direct numerical reconstruction of conductivities in three dimensions**

In: Inverse Problems, vol.: 27, pp. 015002 (2011). Institute of Physics Publishing.

Knudsen, Lars Ramkilde; Miolane, Charlotte Vikkelsø

**Counting equations in algebraic attacks on block ciphers**

In: International Journal of Information Security, vol.: 9(2), pp. 127-135 (2010). Springer.

Knudsen, Lars Ramkilde; Mathiassen, John Erik; Muller, Frédéric; Thomsen, Søren Steffen

**Cryptanalysis of MD2**

In: Journal of Cryptology, vol.: 23(1), pp. 72-90 (2010). Springer New York LLC.

Kokkendorff, Simon Lyngby; Starke, Jens; Hummel, N.

**Interacting many-particle systems of different particle types converge to a sorted state**

In: S I A M Journal on Applied Mathematics, vol.: 70(7), pp. 2534-2555 (2010). Society for Industrial and Applied Mathematics.

Kreissl, Sebastian; Pingen, Georg; Evgrafov, Anton; Maute, Kurt

**Topology optimization of flexible micro-fluidic devices**

In: Structural and Multidisciplinary Optimization, vol.: 42(4), pp. 495-516 (2010). Springer.

Le, T.H.A.; Pham, D. T.; Canh, Nam Nguyen; Le, D.M.

**Methods for optimizing over the efficient and weakly efficient sets of an affine fractional vector optimization program**

In: Optimization, vol.: 59(1), pp. 77-93 (2010). Taylor & Francis Ltd.

Leander, Gregor; Bracken, Carl

**A highly non-linear differentially 4 uniform power mapping that permutes fields of even degree**

In: Finite Fields and Their Applications, vol.: 16(4), pp. 231-242 (2010). Academic Press.

Lin, Z.G.; Pedersen, Michael; Zhang, Lai

**A predator-prey system with stage-structure for predator and nonlocal delay**

In: Nonlinear Analysis: Theory, Methods & Applications, vol.: 72(3-4), p.p. 2019-2030 (2010). Pergamon.

Lin, Zhigui; Liu, Jiahong; Pedersen, Michael  
**Periodicity and blowup in a two-species cooperating model**

In: Nonlinear Analysis: Real World Applications, vol.: 12(1), pp. 479-486 (2011). Elsevier Ltd.

Markvorsen, Steen; Palmer, Vicente

**Extrinsic Isoperimetric Analysis on Submanifolds with Curvatures bounded from below**

In: Journal of Geometric Analysis, vol.: 20, pp. 388-421 (2010). Springer New York LLC.

Nguyen, Dang Manh; Evgrafov, Anton; Gersborg, Allan Roulund; Gravesen, Jens

**Isogeometric Shape Optimization of Vibrating Membranes**

In: Computer Methods in Applied Mechanics and Engineering (2010). Elsevier BV.

Pedersen, Johan Rønby; Aref, Hassan

**Chaos in body-vortex interactions**

In: Proceedings of The Royal Society of London Series A - Containing Papers of a Mathematical and Physical Character, vol.: 466(2119), pp. 1871-1891 (2010).

Pedersen, Johan Rønby; Aref, Hassan

**On the atmosphere of a moving body**

In: Physics of Fluids, vol.: 22(5), Article no. 057103 (2010). American Institute of Physics.

Pedersen, Michael; Lin, Zhigui; Tian, Canrong  
**Traveling wave solutions for reaction-diffusion systems**

In: Nonlinear Analysis: Theory, Methods & Applications, vol.: 73 (2010). Pergamon.

Pingen, Georg; Waidmann, Matthias; Evgrafov, Anton; Maute, Kurt

**A parametric level-set approach for topology optimization of flow domains**

In: Structural and Multidisciplinary Optimization, vol.: 41(1), pp. 117-131 (2010). Springer.

Rasmussen, Anders Rønne; Sørensen, Mads Peter; Gaididei, Yuri Borisovich; Christiansen, Peter Leth

**Interacting Wave Fronts and Rarefaction Waves in a Second Order Model of Nonlinear Thermoviscous Fluids : Interacting Fronts and Rarefaction Waves**

In: Acta Applicandae Mathematicae (2010). Springer Science+Business Media B.V.

Stolpe, Mathias

**On some fundamental properties of structural topology optimization problems**

In: Structural and Multidisciplinary Optimization, vol.: 41(5), pp. 661-670 (2010). Springer.

Thomassen, Carsten

**Spanning trees and orientations of graphs**

In: The Journal of Combinatorics, vol.: 1(2), pp. 101-111 (2010). International Press.

Willatzen, M.; Gravesen, Jens; Voon, L. C. Lew Yan

**Analytic theory of curvature effects for wave problems with general boundary conditions**

In: Physical Review A (Atomic, Molecular and Optical Physics), vol.: 81(6), Article no. 060102 (2010). American Physical Society.

Willatzen, M.; Gravesen, Jens

**Electron conductance in curved quantum structures**

In: Superlattices and Microstructures, vol.: 47(1), pp. 202-206 (2010). Academic Press.



**4.1.1 Articles in Journals, not reviewed**

Hansen, Vagn Lundsgaard

**Med ånden i hånden**

In: Håndarbejde i Skolen, vol.: 45(4), pp. 43-47 (2010). Danmarks Håndarbejds lærerforening.

Hansen, Vagn Lundsgaard; Hjorth, Poul G.

**Tal og geometri på date - giver Abelpris til Tate**

In: Aktuel Naturvidenskab (6), pp. 40-42 (2010).



**4.2 Conference Papers published in Journals, peer reviewed**

Mijatovic, Nenad; Abrahamsen, Asger Bech; Træholt, Chresten; Seiler, Eugen; Henriksen, Mogens; Rodriguez Zermeno, Victor Manuel; Pedersen, Niels Falsig

**Superconducting generators for wind turbines: design considerations**

Presented at: The European Conference on Applied Superconductivity. Dresden (Germany), 2009

In: Journal of Physics: Conference Series (Online), vol.: 234(3), Article no. 032038 (2010). Institute of Physics Publishing.



**4.3 Conference Papers published in Books/Proceedings, peer reviewed**

Bagheri, Nasour; Gauravaram, Praveen; Naderi, Majid; Thomsen, Søren Steffen

**On the Collision and Preimage Resistance of Certain Two-Call Hash Functions**

Presented at: Cryptology And Network Security. Kuala Lumpur, Malaysia, 2010.

In: Proceedings of the 9th International Conference on Cryptology and Network Security, 6467: Springer, 2010 (pp. 96-105).

Borghoff, Julia; Knudsen, Lars Ramkilde; Matusiewicz, Krystian

**Analysis of Trivium by a Simulated Annealing variant**

Presented at: ECRYPT workshop on Tools for Cryptanalysis 2010. Royal Holloway, University of London, Egham, UK, 2010.

In: Proceedings of the ECRYPT workshop on tools in cryptanalysis 2010 / Editor: Standaert, Francois-Xaver.

Gauravaram, Praveen; Leurent, Gaëtan; Mendel, Florian; Plasencia, Maria Naya; Peyrin, Thomas; Rechberger, Christian; Schläffer, Martin

**Cryptanalysis of the 10-Round Hash and Full Compression Function of SHAvite-3-512**

Presented at: International Conference on Cryptology in Africa, 2010.

In: AFRICACRYPT 2010 / Editor: Bernstein, Daniel J.; Lange, Tanja: Springer, 2010 (pp. 419-436).

Hjorth, Poul G.; Allwright, David; Curtis, Mark; Lengiewicz, Jakub

**“Structural models for wind turbines”**

Report of the 73rd European Study Group with Industry, University of Warwick, U.K.

Inagaki, Mizuho; Kawamoto, Atsushi; Abekura, Takanori; Suzuki, Atsushi; Ruebel, Jan; Starke, Jens

**Coupling Analysis of Dynamics and Oil Film Lubrication on a Rotor - Floating Bush Bearing System**

Presented at: Asian Conference on Multibody Dynamics, 2010.

In: ACMD 2010 - Kyoto, Japan, 2010.

Karamehmedovic, Mirza; Sørensen, Mads Peter; Hansen, Poul-Erik; Lavrinenko, Andrei

**Application of the method of auxiliary sources in optical diffraction microscopy**

Presented at: European Consortium for Mathematics in Industry 2008 Conference. London, UK, 2008

In: Progress in Industrial Mathematics at ECMI 2008 - 1 ed. - Heidelberg, Dordrecht, London, New York: Springer, 2010 (pp. 899-905).

Kumar, Ashish; Sanadhya, Somitra Kumar; Gauravaram, Praveen; Safkhani, Masoumeh; Naderi, Majid

**Cryptanalysis of Tav-128 hash function**

Presented at: Indocrypt 2010, 2010.

In: Proceedings of Indocrypt 2010: 11th International Conference on Cryptology in India / Editor: Gong, Guang; Gupta, Kishan Chand: Springer, 2010 (pp.118-130).

Mendel, Florian; Rechberger, Christian; Schläffer, Martin; Thomsen, Søren Steffen

**Rebound Attacks on the Reduced Grøstl Hash Function**

Presented at: CT-RSA, 2010.

In: Topics in Cryptology - CT-RSA 2010: Springer Verlag, 2010 (pp. 350-365).

Mijatovic, Nenad; Rodriguez Zermeno, Victor Manuel; Træholt, Chresten; Zirngibl, Thomas; Seiler, Eugen; Abrahamsen, Asger Bech; Pedersen, Niels Falsig; Sørensen, Mads Peter

**Towards faster FEM simulation of thin film superconductors**

Presented at: ECMI 2010 Conference. Wuppertal, Germany, 2010.

In: ECMI 2010 Conference.

Mouha, Nicky; Sekar, Gautham; Aumasson, Jean-Philippe; Peyrin, Thomas; Thomsen, Søren Steffen; Turan, Meltem Sönmez; Preneel, Bart

**Cryptanalysis of the ESSENCE Family of Hash Functions**

Presented at: International Conference of Information Security and Cryptology. Beijing, China,

2009.

In: Information Security and Cryptology: 5th International Conference, Inscrypt 2009, Beijing, China, December 12-15, 2009. Revised Selected Papers: Springer, 2010 (pp. 15-34).

Nguyen, Dang Manh; Evgrafov, Anton; Gravesen, Jens; Jensen, Jakob Søndergaard

**Isogeometric Analysis Towards Shape Optimization in Electromagnetics**

Presented at: Nordic Seminar on Computational Mechanics. Stockholm, 2010.

In: Proceedings of NSCM-23, the 23rd Nordic Seminar on Computational Mechanics - Stockholm, 2010 (pp.18-21).

Rasmussen, Anders Rønne; Sørensen, Mads Peter; Gaididei, Yuri Borisovich; Christiansen, Peter Leth

**Analytical and numerical modelling of thermoviscous shocks in their interactions in nonlinear fluids including dissipation.**

Presented at: European Consortium for Mathematics in Industry 2008 Conference. London, UK, 2008.

In: Progress in Industrial Mathematics at ECMI 2008 - 1 ed. - Heidelberg, Dordrecht, London, New York: Springer Verlag, 2010 (pp.997-1002).

Rodriguez Zermeno, Victor Manuel; Sørensen, Mads Peter; Pedersen, Niels Falsig; Mijatovic, Nenad; Abrahamsen, Asger Bech

**Fast 2D Simulation of Superconductors: a Multiscale Approach**

Presented at: COMSOL Conference 2009. Milan, Italy, 2009.

In: Proceedings of the COMSOL Conference 2009, Milano, Italy; User presentations and proceedings CD: COMSOL Inc., 2009.

Schmidt, Karsten; Rattleff, Pernille; Hussmann, Peter Munkebo

**The Impact of CAS Use in Introductory Engineering Mathematics**

Presented at: ECMI 2008

In: Progress in Industrial Mathematics at ECMI 2008 Springer, 2010.

Thomsen, Søren Steffen

**Pseudo-cryptanalysis of the Original Blue Midnight Wish**

Presented at: Fast Software Encryption. Seoul, Republic of Korea, 2010.

In: Fast Software Encryption 2010: Springer, 2010 (pp.304-317).



**4.3.1 Conference Papers published in Books/Proceedings, not reviewed**

Gravesen, Jens; Evgrafov, Anton; Gersborg, Allan Roulund; Nguyen, Dang Manh; Nielsen, Peter Nørtoft

**Isogeometric analysis and shape optimisation**

Presented at: Nordic Seminar on Computational Mechanics, Stockholm, 2010.

In: Proceedings of NSCM-23: the 23rd Nordic Seminar on Computational Mechanics / Editor: Erikson, Anders; Tibert, Gunnar, 2010 (pp.14-17).



**4.4 Conference/Meeting contributions (posters, abstracts etc.), peer reviewed**

Amir, Oded; Stolpe, Mathias; Sigmund, Ole  
**Efficient computational procedures for topology optimization of nonlinear structures**

Conference abstract presented at: European Conference on Computational Mechanics. Paris, France, 2010.

Dankowicz, Harry; Schilder, Frank  
**A Multi-Point, Boundary-Value Problem, Collocation Toolbox for the Continuation of sets of Constrained Orbit Segments**

Conference abstract presented at: US National Congress of Theoretical and Applied Mechanics. State College, Pennsylvania, USA, 2010.

Evgrafov, Anton; Gregersen, Misha Marie; Sørensen, Mads Peter

**Cell based finite volume discretization of control in the coefficients problems**

Conference abstract presented at: 23rd Nordic Seminar on Computational Mechanics. Stockholm, Sweden, 2010

In: Proceedings of NSCM-23: the 23rd Nordic Seminar on Computational Mechanics, pp. 306-309 / Editor: Eriksson, Anders; Tibert, Gunnar - Stockholm, Sweden: KTH Mechanics, 2010.

Evgrafov, Anton; Berggren, Martin

**Topology optimization using a discontinuous Galerkin method**

Conference abstract presented at: International Conference on Engineering Optimization. Lisbon, Portugal, 2010.

Gauravaram, Praveen

**Cryptanalysis of Tav-128 hash function**

Slide show presentation presented at: Indocrypt 2010. Hyderabad, India, 2010

In: Indocrypt 2010; 6498, p. 118-130 / Editor: Gong, Guang; Gupta, Kishan Chand, Springer, 2010.

Gauravaram, Praveen

**Fixing non-randomness in PGVs**

Slide show presentation presented at: CRYPTO 2010. University of California, Santa Barbara, 2010.

Gauravaram, Praveen

**How good are some 2nd round SHA3 hashes when their compression functions are weak?**

Slide show presented at: CRYPTO 2010. University of California, Santa Barbara, 2010.

Nguyen, Dang Manh; Evgrafov, Anton; Gersborg, Allan Roulund; Gravesen, Jens

**Isogeometric Shape Optimization of Vibrating Membranes**

Slide show presented at: IV European Conference on Computational Mechanics. Paris, France, 2010.

Nguyen, Dang Manh; Evgrafov, Anton; Gersborg, Allan Roulund; Gravesen, Jens

**Isogeometric Shape Optimization of freely varying shapes**

Conference abstract presented at: 9th World Congress on Computational Mechanics and 4th Asian Pacific Congress on Computational Mechanics. Sydney, Australia, 2010.

Røgen, Peter; Koehl, Patrice

**A smooth knowledge based potential for protein structure refinement**

Poster presentation at: European Conference on Computational Biology. Ghent, Belgium, 2010.

Starke, Jens

**Deterministic and stochastic modelling of catalytic surface processes**

Invited plenary talk at: Ertl Symposium. Gwangju, South Korea, 2010.



**4.4 1. Conference contributions (posters, abstracts etc.), not reviewed**

Abrahamsen, Asger Bech; Seiler, Eugen; Mijatovic, Nenad; Jensen, Bogi Bech; Zirngibl, Thomas; Træholt, Chresten; Henriksen, Mogens; Nørgård, Per Bromand; Lystrup, Aage; Jacobsen, Claus Schelde; Hansen, Jørn Bindslev; Grivel, Jean-Claude; Mozhaev, Peter; Zermeno, Victor Manuel Rodriguez; Sørensen, Mads Peter; Pedersen, Niels Falsig; Andersen, Niels Hessel; Østergaard, Jacob

**Superconducting wind turbines**

Slide show presented at: Dutch Power Innovation Day. Twente (NL), March 11, 2010.

Gregersen, Misha Marie

**Topology optimization of heat conduction problems**

Lecture presented at FlowHEAD 18M meeting and workshop on industrial design optimization for fluid flow, Varna, Bulgaria, September 20-24, 2010.

Jensen, Bogi Bech; Seiler, Eugen; Mijatovic, Nenad; Zermeno, Victor Manuel Rodriguez

**Multi-Pole HTS Generators for Direct Drive Wind Turbines**

Conference abstract presented at: Nordic Conference on Magnet Technology. Tampere, Finland, 2010.

Munoz, Eduardo; Stolpe, Mathias

**Global Optimal Design of Composite Laminates Including Failure Criteria Using Decomposition Techniques**

Conference abstract presented at: IV European Conference on Computational Mechanics. Paris, France, 2010.

In: ECCOMAS-2010 Proceedings/Corresponding author: Munoz, Eduardo, 2010.

Nguyen, Dang Manh; Evgrafov, Anton; Gersborg, Allan Roulund; Gravesen, Jens

**Isogeometric Design of Vibrating Membranes**

Slide show presented at: New Trends in Applied Geometry. Bad Herrenalb, Germany, 2010.

Nielsen, Peter Nørtoft; Gersborg, Allan Roulund; Gravesen, Jens; Pedersen, Niels Leergaard  
**Isogeometric Analysis and Shape Optimiza-**

**tion for Fluids**

Slide show presented at: SIAMUW Graduate Student Seminar. University of Washington, Seattle, Washington, USA, 2010.

Nielsen, Peter Nørtoft; Gersborg, Allan Roulund; Gravesen, Jens; Pedersen, Niels Leergaard  
**Isogeometric Analysis and Shape Optimization for Fluids**

Slide show presented at: Applied Math Seminar at Boeing Research & Technology. Bellevue, Washington, USA, 2010.

Nielsen, Peter Nørtoft; Gersborg, Allan Roulund; Gravesen, Jens

**Isogeometric Analysis and Shape Optimization in Fluid Mechanics**

Slide show presented at: IV European Conference on Computational Mechanics. Paris, France, 2010.

Nielsen, Peter Nørtoft; Gersborg, Allan Roulund; Gravesen, Jens

**Isogeometric Analysis and Shape Optimization in Stokes Flow Problems**

Slide show presented at: New Trends in Applied Geometry. Bad Herrenalb, Germany, 2010.

Nielsen, Peter Nørtoft; Nguyen, Dang Manh; Evgrafov, Anton; Gersborg, Allan Roulund; Gravesen, Jens

**Isogeometric Shape Optimization**

Slide show presented at: Non-Standard Numerical Methods for PDE's. Pavia, Italy, 2010.

Stolpe, Mathias

**Solving the Zhou-Rozvany Problem**

Poster presentation at: DCSC User Conference 2010. Copenhagen Airport, Denmark, 2010.

Sørensen, Mads Peter

**Non negativity of concentrations in reaction diffusion advection models, exemplified by the blood coagulation cascade.**

Talk at minisymposium: Web-supported education within industrial mathematics and nanoelectronics industry.

Sørensen, Mads Peter; Zermeno, Victor Manuel Rodriguez

**Towards faster FEM simulation of thin film superconductors: a multiscale approach.**

Poster presented at ECMI 2010 Conference, Bergische Universität Wuppertal, Germany, July 26-30, 2010.



#### 4.5 Chapters in Books, peer reviewed

Christensen, Ole; Feichtinger, Hans; Paukner, Stephan

##### **Gabor analysis for imaging**

In: Handbook in Imaging: Springer, 2010

Gauravaram, Praveen; Knudsen, Lars Ramkilde

##### **Cryptographic Hash Functions**

In: Handbook of Information and Communication Security / Editor: Stavroulakis, Peter; Stamp, Mark - 1 ed. - Berlin Heidelberg: Springer Verlag, 2010.



#### 4.6 Books

Christensen, Ole

##### **Functions, Spaces, and Expansions**

Birkhaeuser , 2010.



#### 4.7 Reports, peer reviewed

Hurtado, Ana; Markvorsen, Steen; Palmer, Vicente

##### **Comparison of Exit Time Moment Spectra for Extrinsic Metric Balls**

DTU Mathematics, 2010 (p. 15)

In: Mat-Report; 2010-0.

Gauravaram , Praveen and Thomsen, Søren S. Contribution to D.SYM.4 SHA-3 Design and Cryptanalysis Report. European Network of Excellence in Cryptology II (ECRYPT II), ICT-2007-216676, August 2010. Report published at [www.ecrypt.eu.org/documents/D.SYM.4.pdf](http://www.ecrypt.eu.org/documents/D.SYM.4.pdf).



#### 4.7.1 Reports, not reviewed

Christensen, Ole; Powell, Alexander; Xiao, Xiangchun

##### **A note on finite dual frame pairs**, 2010.

Christensen, Ole; Xiao, Xiangchun; Zhu, Yu Can

##### **Characterizing R-duals in Banach spaces**, 2010.

Christensen, Ole; Sielemann Jakobsen, Mads

##### **Dual pairs of Gabor frames for generators without the partition of unity property**. 2010.

Christensen, Ole; Massopust, Peter

##### **Exponential B-splines and the partition of unity property**, 2010.

Christensen, Ole; Kim, Hong Oh; Rae Young, Kim

##### **Gabor windows supported on [-1,1] and dual windows with short support**, 2010.

Christensen, Ole; Kim, Hong Oh; Kim, Hong Oh

##### **On the duality principle by Casazza, Kutyniok and Lammers**, 2010.



#### 4.8 Academic Dissertations, peer reviewed

Brander, Kristian

##### **Interpolation and List Decoding of Algebraic Codes**

PhD Thesis; Technical University of Denmark (DTU), Kgs. Lyngby, 2010.

Larsen, Anders Astrup; Hattel, Jesper Henri; Sigmund, Ole

##### **Process optimization of friction stir welding based on thermal models**

PhD Thesis; Technical University of Denmark (DTU), Kgs. Lyngby, 2010 (pp. 110).

Munoz, Eduardo

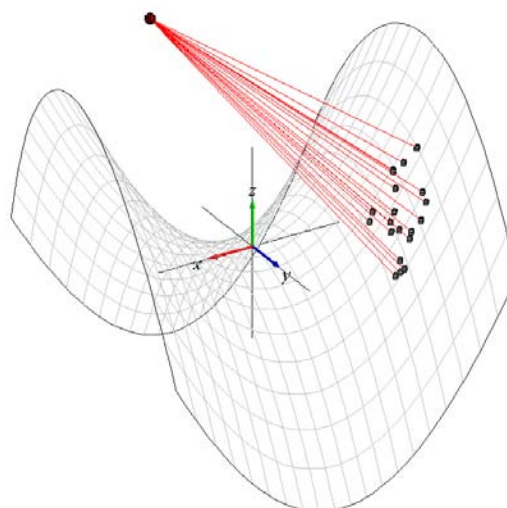
**Global Optimization for Structural Design by Generalized Benders' Decomposition**

PhD Thesis; Technical University of Denmark (DTU), Kgs. Lyngby, 2010 (pp. 169).

Schou, Marie-Louise Højlund

**Topology optimization problems with design-dependent sets of constraints**

PhD Thesis; Technical University of Denmark (DTU), Kgs. Lyngby, 2010 (pp. 213).



**4.8.1 Academic Dissertations, not reviewed**

Amir, Oded; Sigmund, Ole

**Efficient Analysis Procedures in Structural Topology Optimization**

PhD Thesis; Technical University of Denmark (DTU), Kgs. Lyngby, Denmark: 2010 (p. 151).



**4.9. Lecture Notes**

Markvorsen, Steen

**Integration i flere variable**

Presented at: 01005 Matematik 1, 2010.



**4.10 Miscellaneous**

Andersen, Kurt Munk; Sandqvist, Allan

**A generalized Allwright formula and the vector Riccati equation**

Article at website in: ArXiv (2010).

**5. Research collaboration**

**5.1 Projects funded by external sources**

**5.1.1 ECRYPT II**

“European Network of Excellence for Cryptology II” is a 4-year network of excellence funded within the Information & Communication Technologies (ICT) Programme of the European Commission's Seventh Framework Programme (FP7) under contract number ICT-2007-216676. Participants from DTU Mathematics: Lars R. Knudsen, Søren Steffen Thomsen, Erik Zenner, Julia Borghoff, Praveen Gauravaram, Gregor Leander, Krystian Matusiewicz, Valerie Umana Gauthier.

**5.1.2 MECOBS**

Project with other Danish Universities. Leader Michael Pedersen. Other DTU Mathematics participants: Mads P. Sørensen, Morten Brøns, Ole Christensen, Martin P. Bendsøe and Kim Knudsen. Involves also Biocentrum DTU, BioSim DTU and DTU AQUA.

**5.1.3 Fluid-DTU**

Center for Fluid Dynamics is a research collaboration between DTU departments, comprising FYS, MEK, KT, MIC and MAT. The center holds a grant from the Danish National Research Foundation for a five-year Niels Bohr visiting professorship. DTU Mathematics participants: Morten Brøns (member of the steering committee) Poul G. Hjorth, Mads Peter Sørensen, Christian Henriksen, Jens Starke.

**5.1.4 Danish Centre for Composite Structures and Materials for Wind Turbines (DCCSM)**

This research centre is funded by the Danish Council for Strategic Research's Programme Commission on Energy and Environment. The centre runs from 2010 to 2017. The partners in the centre include Risø DTU (Materials Research Division & Wind Energy Division), DTU Mechanical Engineering, Department of Mechanical Engineering at Aalborg University, DTU Civil Engineering, DTU Nanotech, DTU Mathematics, Siemens Wind Power, LM Glasfiber, Fiberline Composites, Bach Composite Industry. The centre homepage is [www.dccsm.dk](http://www.dccsm.dk)  
DTU Mathematics participants: Mathias Stolpe and Alemseged Gebrehiwot Weldeyesus.

**5.1.5 "Geometric Analysis"**

Research project with Vicente Palmer (Project Manager) and Ana Hurtado, Universitat Jaume I, Castellon, Spain. Funded by the Spanish Ministry of Science. Participant from DTU Mathematics: Steen Markvorsen.

**5.1.6 CODY**

European Research Training Network on Conformal Structures and Dynamics. 4-year project funded by EU FP6. Participants from DTU Mathematics: Bodil Branner, Christian Henriksen.

**5.1.7 "Complex Methods in Dynamical Systems and Special Functions"**

FNU research grant. With Christian Berg and Henrik Laurberg Pedersen, Copenhagen University and Carsten Lunde Petersen, Roskilde University. Participant from MAT: Christian Henriksen.

**5.1.8 "Algebraic Coding Theory"**

FNU research grant. Participants from MAT: Peter Beelen, Tom Høholdt.

**5.1.9 "Equation-free analysis of mechanical vibrations"**

Project with I. Santos and J.J. Thomsen, Department of Mechanical Engineering, DTU. 3-year project funded by FTP. Participant from MAT: and principal investigator: Jens Starke.

**5.1.10 "E-learning in Mathematics 1 (cf. 3.5)"**

Participants: DTU Informatics, DTU Mathematics and LearningLab DTU. The project is funded by the Ministry of Science, Technology, and Innovation via the National IT and Telecom Agency. Participants from DTU Mathematics: Steen Markvorsen and Karsten Schmidt.

**5.1.11 Solar collectors**

The aim of this Matematicum project is to design laboratory experiments with solar collectors and to develop the appropriate mathematical models. The project is funded by Den Danske Bank. Participants from MAT: Karsten Schmidt, Steen Markvorsen.

**5.1.12 Fluid optimization workflows for high effective automotive development processes (FlowHEAD), EU Seventh Framework Programme of the European Community for Research, Technological Development and Demonstration Activities under the funding scheme of "Collaborative Project"**

Project with Queen Mary College, London, UK (Coordinator); CD-adapco, Paris, France; DTU Mechanics, Kgs. Lyngby, Denmark; ESI-group, Paris, France; FE-Design, Karlsruhe, Germany; ICON, Berkshire, UK; Renault, France, TU München, Germany; Technical University of Sofia, Bulgaria; Volkswagen AG, Wolfsburg, Germany; Warsaw University of Technology, Poland. Amount to DTU Mathematics: 332.768 Euro. Participants from DTU Mathematics: Anton Evgrafov and Mads Peter Sørensen. From DTU Mechanics: Allan Roulund Gersborg.

**5.1.13 Nanomechanical sensors and actuators, fundamentals and new directions (NAMEC)**

Villum Kann Rasmussen Centre of Excellence. Project with DTU Nanotech (Professor Anja Boisen, head of centre), DTU Electrical Engineering, and Pharmaceutical Faculty, University of Copenhagen. Amount to DTU Mathematics: 3.082.000 DKK. (Total budget 28 MDKK). Participants from DTU Mathematics: Anton Evgrafov and Mads Peter Sørensen.

**5.1.14 Post-quantum cryptology**

Project with Aarhus University, Ivan B. Damgård. Funded by the Villum Kann Rasmussen Foundation. Participants from MAT: Lars R. Knudsen, Gregor Leander, Søren S. Thomsen, Valerie Gauthier Umana.

**5.1.15 Cryptanalysis by means of Numerical Methods**

Project with University of Technology, Graz, Austria. Funded by FTP. Participants from MAT: Lars R. Knudsen, Krystian Matusiewicz, Julia Borghoff.

**5.1.16 Matematicum**

Matematicum, the mathematical inspiratorium at DTU (cf. 3.1), is funded by FNU, the Danish Research Agency, The Birch & Krogboe Founda-

tion (Alectia), DTU's Strategic Fund, Danske Bank, the Corrit Foundation, and Skoletjenesten.

### 5.1.17 "Research activities in Discrete Mathematics"

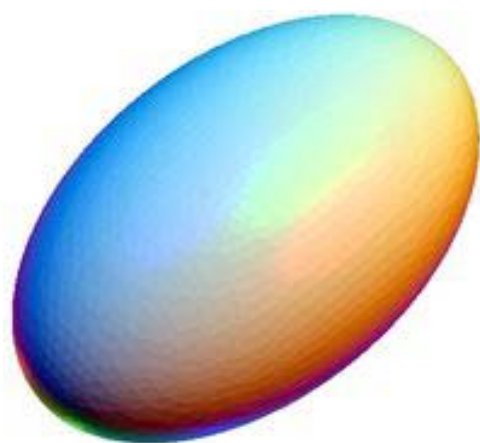
FNU Research Grant 2010-2012. Participant from MAT: Carsten Thomassen.

### 5.1.18 Graphs on higher surfaces

This project is a collaboration between Dr. Ken-ichi Kawarabayashi, National Institute of Informatics, National Center of Science, Japan, and Professor Carsten Thomassen, DTU MAT, concerning extendability of results on planar graphs to higher surfaces. The project is supported (in the form of travel expenses) by FNU (Rammebevilling i Diskret Matematik) and National Center of Science, Tokyo, Japan.

### 5.1.19 "Reconstruction Methods for 3D Electrical Impedance Tomography"

Post doc grant funded by the Villum Kann Rasmussen foundation: Kim Knudsen.



## 5.2 Other collaborative projects

### Brander, David

- With J. Dorfmeister, TU Munich, Germany, on integrable systems methods in geometry.
- With Martin Svensson, University of Southern Denmark, on integrable systems and bi-harmonic maps.

### Branner, Bodil

- With Núria Fagella, Universitat de Barcelona, Spain. On quasi-conformal surgery.

### Brøns, Morten

- With K. Hourigan, M. Thompson, D. Lo Jacomo and G. Sheard, Monash University, Melbourne, Australia. On topological analysis of flow structures in vortex flows and bluff body wakes.
- With Eduardo Ramos, Sergio Cuevas and Alberto Beltrán, Universidad Nacional Autónoma de México. On flow topology in magnetically driven flows.

### Christensen, Ole

- With Rae Young Kim, Yeungnam University. On discrete Gabor systems and their applications
- With Say Song Goh, National University of Singapore: Periodic Wavelet Frames.
- With Hong Oh Kim, KAIST, and Rae Young Kim, Yeungnam University, South Korea: On an abstract duality concept.
- With Peter Massopust, TU Munich, Germany: Dual Gabor frames without the partition of unity property
- With Powell, Alex, Vanderbilt University, USA and Xiangchung Xiao, Xiamen University, China: Finite-dimensional frames.

### Gravesen, Jens

- With B. Jüttler, Johannes Kepler University, Linz, Austria, and Z. Šír, Charles University in Prague, Czech Republic. Curves and Surfaces represented by Support Functions.
- With M. Willatzen, University of Southern Denmark. Sønderborg, Denmark. Geometrical effects in Quantum Mechanics.
- With S. Markvorsen, H. Almegaard and A. Bagger, DTU Civil Engineering, B. Jüttler, Johannes Kepler University, Linz, Austria, and Z. Šír, Charles University in Prague, Czech Republic. Faceting of surfaces.
- With C. Henriksen, Jihong Wang, University of Birmingham, England. Scroll modelling.
- With A. Evgrafov, D.M. Nguyen. P.M. Nielsen, and A.R. Gersborg DTU Mechanical Engineering. Isogeometric Analysis.

### Hansen, Vagn Lundsgaard

- Editor for the volume "History of Mathematics" for "Encyclopedia of Life Support Systems" (EOLSS) developed under the auspices of the UNESCO, with Jeremy Gray, Open University, UK, as co-editor.

### Hjorth, Poul G.

- With D.D. Holm, Department of Mathematics, Imperial College, London.
- With T. Schmidt, Danish Meteorological Institute.

### *Høholdt, Tom*

- With H. Janwa, University of Puerto Rico, Puerto Rico. On codes and expander graphs.
- With S. Ghorpade, Indian Institute of Science, Mumbai, India. On Affine Grassmann Codes.
- With J. Justesen, Washington, USA. On codes from graphs.

### *Markvorsen, Steen*

- With G. Pacelli Bessa and J. Fabio Montenegro, Fortaleza, Brazil. On heat kernel comparison theorems.
- With Jacob Vedelsby, Denmark, concerning translation of contributions to RPA/EMS website.

### *Schilder, Frank*

- With Harry Dankowicz, UIUC, Illinois, USA; David Barton, University of Bristol, UK: MATLAB toolbox for numerical bifurcation analysis.
- With Claudia Wulff, University of Surrey, UK: Numerical bifurcation analysis of Hamiltonian relative periodic orbits.
- With Jan Sieber, University of Portsmouth, UK; David Barton: control based continuation in experiments

### *Schmidt, Karsten*

- With Pernille Rattleff (DPU) and Peter M. Hussmann (Learning Lab DTU): How do the students use textbooks and other knowledge resources in relation to different study activities.
- With Anne Marie Holm and Bjørn Petersen, Lyngby Tekniske Gymnasium, and Ulrik Englund Petersen, DTU Mathematics. Bridge-building from high school to university.

### *Starke, Jens*

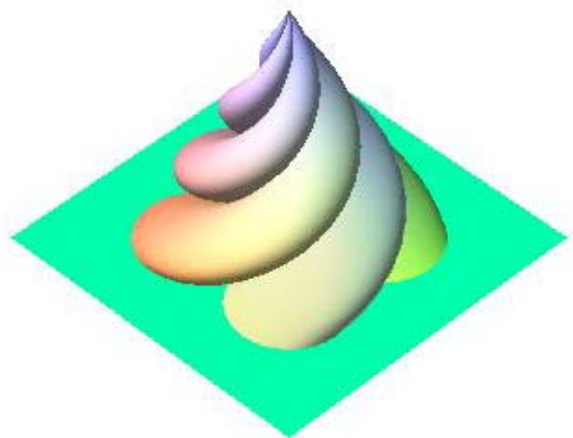
- With J. Midtgaard, University of Copenhagen, C. Ellsaesser and T. Kuner, University of Heidelberg, Germany. Analysis of macroscopic phenomena on the neural network in the olfactory bulb.
- With M. Schanz, University of Stuttgart, Robust algorithms for robot soccer and other distributed robotic systems.
- With Y. Gaididei, University of Kiev, Ukraine, on travelling waves in traffic systems.
- With Jan Sieber, University of Portsmouth, UK, on bifurcation analysis for experiments.

### *Sørensen Mads Peter*

- With Jean-Guy Caputo, University of Rouen, France. Project on sine-Gordon systems and traffic models.
- With Niels Falsig Pedersen and Nenad Mijatovic, DTU Electrical Engineering, Asger Abrahamsen, Risø-DTU, Anbarasu, Ramasamy, Vestas Technology R&D, Superwind.
- With Yuri Gaididei, University of Kiev, Ukraine. Project on thermo viscous fluids and shock waves, traffic models and conformational transformations of biomolecules.
- With Carlos Gorria, Department of Applied Mathematics and Statistics, University of the Basque Country, Bilbao, Spain. Project on conformational transformations of biomolecules.
- With Messoud Efendiev, Department of Dynamical Systems, Institute of Biomathematics and Biometry, Helmholtz Zentrum München, Germany. Project on reaction diffusion advection equations.
- With Jesper Mygind, DTU Physics. Cosupervision of Ph.D. student Anna Gordeeva.

### *Thomassen, Carsten*

- With Ken-ichi Kawarabayashi, Tohoku University, Japan. On the chromatic number of graphs on surfaces
- With Andre Kundgen, California State University San Marcos. Quadrangulations in triangulations of graphs on surfaces.
- With Andre Kundgen, California State University San Marcos, and Gregor Leander DTU. Central digraphs.



## 6. Conference participation

*Abdelraheem, Mohamed Ahmed*

- RFIDSec2010, Istanbul, June 2010.

*Beelen, Peter*

- The Claude Shannon Institute Workshop on Coding and Cryptography, Cork, Ireland. Title of talk: “List decoding algebraic geometry codes with Alekhovich’s algorithm”. May 17-18, 2010.
- RISC/Intercity number theory seminar on Crypto, Coding and Geometry, Amsterdam, Holland. Title of talk (invited): “Obtaining information about explicit towers using their modular interpretation”. November 18-19, 2010.
- May 10-13, November 20-26, December 17-24, 2010: Visit to CWI, Amsterdam, the Netherlands.

*Borghoff, Julia*

- ECRYPT workshop on Tools for Cryptanalysis, June 22-23, 2010, Egham, UK. Title of the given talk: “Analysis of Trivium by a simulated annealing variant.”
- SCC 2010, 2<sup>nd</sup> Conference on Symbolic Computation and Cryptography, June 23-25, 2010, Egham, UK
- SAC 2010, Selected areas in Cryptography, August 12-13, 2010, Waterloo, Canada, Title of the given talk: “Hill climbing algorithms and Trivium”.
- 30th International Cryptology Conference (CRYPTO 2010), Santa Barbara, USA.

*Brander, David*

- First International Conference on Math. and Statistics, Sharjah, March 2010. (Invited talk).
- Differential Geometry and its Applications, Brno, Czech Republic, August 2010. (Invited talk).
- 3rd Odense Winter School on Geometry and Theoretical Physics, USD, Odense, November 2010. Attended.

*Branner, Bodil*

- British Women in Maths Meeting and EMS committee on Women in Maths Meeting, April 15-16, 2010, the Isaac Newton Institute, Cambridge, UK.
- The 8<sup>th</sup> AIMS International Conference on Dynamical Systems, Differential Equations

and Applications, May 25-28, 2010, Dresden, Germany.

- DMF’s sommertræf for kandidatstuderende i matematik, August 12, 2010, Sømminestationen, Holbæk, Denmark.
- Workshop on Holomorphic Dynamics around Thurston’s Theorem, September 27- October 1, 2010, RUC, Denmark.
- Workshop for Women in Maths in Denmark, October 6-7, 2010, Sømminestationen, Holbæk, Denmark.
- Conformal Dynamics and Hyperbolic Geometry. A conference in honor of Linda Keen’s 70<sup>th</sup> birthday, October 21-23, 2010, CUNY Graduate Center, New York, US.

*Christensen, Ole*

- Optimal frames and operator algebras, San Francisco, USA. January 17-20. Talk: A survey on duality in frame theory.
- Conference in Honor of Pete Casazza’s 65th Birthday, May 19-23: Talk: May 30, 1995 – the day Pete entered frame theory.
- MULAC-meeting, June 15, Acoustic Research Institute, Vienna, Austria. Talk: Frames and unbounded operators.

*Gauravaram, Praveen*

- Eurocrypt 2010, 29th International Cryptology Conference. Monaco and Nice, French Riviera. May 30-June 3, 2010.
- Crypto 2010, 30th International Cryptology Conference. UCSB, Santa Barbara, USA. August 15-19, 2010. Presented 2 talks during the Rump Session of the conference. Title of Talk 1: How good are second round SHA3 hashes when their compression functions are weak? Title of Talk 2: Fixing non-randomness in the PGVs.
- CHES 2010, Workshop on Cryptographic Hardware and Embedded Systems. UCSB, Santa Barbara, USA. August 17-20, 2010.
- The Second SHA3 candidate conference. UCSB, Santa Barbara, USA. August 23-24, 2010.
- Indocrypt 2010, 11th International Conference on Cryptology in India. Hyderabad, December 12- 15, 2010. Presented a talk. Title: Cryptanalysis of Tav-128 Hash Function.

*Gravesen, Jens*

- New Trends in Applied Geometry, February 14-19, 2010, Bad Herrenalb, Germany.
- Industry Challenges in Geometric Modeling, CAD and Simulation, March 25-26, 2010,

## Annual Report 2010 – Department of Mathematics DTU

- Darmstadt, Germany. Talk: "Parametrisation in Isogeometric Analysis"
- ECCM 2010, IV European Conference on Computational Mechanics, May 16-21, 2010, Paris, France. Invited talk in minisymposium on isogeometric analysis: "Parametrisation in Isogeometric Analysis"
  - NSCM 23, 23rd Nordic Conference on Computational Mechanics, October 21-22, 2010, Stockholm, Sweden. Keynote presentation: "Isogeometric Analysis and Shape Optimisation".

### *Hansen, Vagn Lundsgaard*

- Workshop on "Raising the Public Awareness of Mathematics", Óbidos, Portugal, September 26-29, 2010. Talk: Keeping Mathematical Awareness Alive.
- Annual Meeting of the Danish Mathematical Society, Odense, Denmark, December 16, 2010. Talk: Mit liv som matematiker (My life as a mathematician).

### *Henriksen, Christian*

- Participated in the 76th European Study Group with Industry at Technical University of Denmark, August 16-20, 2010.
- Participated in workshop titled Around Thurston's Theorem, Søminestationen Holbæk, September 27- October 1, 2010. Gave the lecture: Implementing Thurston's Algorithm.

### *Hjorth, Poul G.*

- Participated in the 73rd European Study Group with Industry, University of Warwick, UK, April 12-16, 2010.
- Participated in the 75th European Study Group with Industry, University of Limerick, Ireland, June 27-July 2, 2010.
- Organized the 76th European Study Group with Industry, DTU, Kgs. Lyngby, Denmark, August 16-20, 2010.

### *Høholdt, Tom*

- "Affine Grassmann Codes". Lecture presented at: International Workshop on Coding Theory, Allerton, Illinois, USA, September 26-29, 2010.

### *Knudsen, Kim.*

- The 8th AIMS Conference on Dynamical Systems, Differential Equations and Applications Dresden University of Technology Dresden, Germany, May 25-28, 2010. Invited talk

- Summer school on computational solution of inverse problems (FICS 2010), University of Helsinki, Finland, on June 28-July 2, 2010. Minicourse on "D-bar methods for nonlinear inverse problems"
- International conference on Inverse Problems, City University of Hong Kong, December 13-17 2010. Plenary talk.

### *Knudsen, Lars R.*

- Eurocrypt, May 2010, Nice, France.

### *Markvorsen, Steen*

- 3D Printing and additive manufacturing, ATV-SEMAPP, at DTU, May 6, 2010. Presentation: "Applications for Geometric Analysis".
- Geometry Day in Lund, May 12, 2010. Co. Sigmundur Gudmundsson.
- Geometry Workshop. Copenhagen University. June 21 – 25, 2010. Co. T. Colding, K. Grove, E.K. Pedersen.
- RPA/EMS conference: Raising Public Awareness of Mathematics, Obidos, Portugal, Presentation: "From PA(X) to RPAM(X)". September 26-29, 2010.
- Computers and Mathematics, at Copenhagen University, HCØ, October 26, 2010. Presentation: "Licence to Thrill".
- Biblioteksledermødet 2010, Nyborg Strand, Co. Styrelsen for Bibliotek og Medier. Presentation: "Forskningen, Biblioteket, OA, og Universet". November 10, 2010.
- Conference on Open Access. Ministry of Education. December 6, 2010.
- Danish Mathematical Society Annual Meeting. Odense. December 16, 2010.

### *Schilder, Frank*

- 8th American Institute of Mathematical Sciences Conference (AIMS), TU Dresden, Germany, May 25-28, 2010.
- Joint SIAM/RSME-SCM-SEMA Meeting on Emerging Topics in Dynamical Systems and Partial Differential Equations, DSPDEs'10, Barcelona, Spain, May 31-June 4, 2010.
- 16th US National Congress on Theoretical and Applied Mechanics (USNCTAM), Pennsylvania State University, USA, June 27-July 2, 2010.
- 4th Brainmodes Conference on Noise, oscillations and frequency locking in neural systems, DTU Denmark, December 9-11, 2010.

## Annual Report 2010 – Department of Mathematics DTU

### *Schmidt, Karsten*

- MONA-conference 27th October in Middelfart. Presentation: “Innovations based on assessments”.
- Conference at Ministry of Science, Technology and Innovation August 19-20, 2010. Presentation (with Kasper Skårhøj): “Learning of mathematics by E-learning”.
- ECMI 2010, July 26-30, 2010 in Wuppertal, Germany. Presentation: “Web-based learning objects in introductory university mathematics”.

### *Starke, Jens*

- “Deterministic and stochastic modelling of catalytic surface processes. 1st Ertl Symposium in Gwangju, South Korea, invited plenary talk, April 11-14, 2010.
- “Continuation and bifurcation analysis of vibrations in mechanical systems”. Joint SIAM/RSME-SCM-SEMA Meeting: Emerging Topics in Dynamical Systems and Partial Differential Equations, DSPDEs'10, Barcelona, Spain, invited minisymposium talk, May 31-June 4, 2010.
- “Analyzing the influence of the neural network topology on pattern formation”, talk, Dynamics Days Europe, Bristol, UK, September, 6.-10, 2010.

### *Sørensen, Mads Peter*

- ECMI 2010 Conference, Bergische Universität Wuppertal, Germany, July 26-30, 2010. (Contributed talk, minisymposium and poster).
- FlowHEAD 18M meeting and workshop on industrial design optimization for fluid flow, Varna, Bulgaria, September 20-24, 2010.

### *Thomassen, Carsten*

- “Graph decomposition” Plenary lecture at “Combinatorics 2010”, Verbania (Italy), June 28-July 3, 2010.
- “Graph decomposition” Plenary Opening lecture at “18<sup>th</sup> International Symposium Graph Drawing 2010”, Konstanz (Germany), September 12-25, 2010.

### *Thomsen, Søren Steffen*

- Fast Software Encryption 2010, Seoul, Korea. February 7-10, 2010. Presentation of the paper “Pseudo-cryptanalysis of the Original Blue Midnight Wish”.
- CRYPTO 2010, Santa Barbara, CA, USA. August 15-19, 2010.

- Cryptographic Hardware and Embedded Systems (CHES) 2010, Santa Barbara, CA, USA. August 17-20, 2010.
- 2nd SHA-3 Candidate Conference, Santa Barbara, CA, USA. August 23-24, 2010. Presentation of the paper “Deterministic Differential Properties of the BMW Compression Function”.

### *Umaña, Valérie Gauthier*

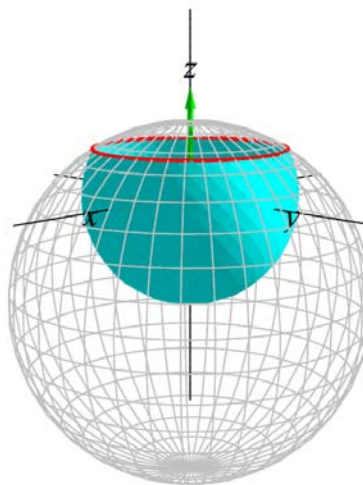
- 2nd International Conference on Symbolic Computation and Cryptography, June 23-25, 2010, Royal Holloway, University of London, Egham – UK. Talk: "Practical Key Recovery Attacks on Two McEliece Variants" With Gregor Leander.

### *Zenner, Erik*

- 2nd “Early Symmetric Crypto” (ESC) Seminar. Remich, LUX, January 11-15, 2010.

### *Zhang, Lai*

- SIAM Conference on the Life Sciences (LS10), The David L. Lawrence Convection Center, Pittsburgh, Pennsylvania, USA, July 12-15, 2010.
- Research visit to The International Institute of Applied System Analysis (IIASA) Vienna, Austria, June 21-July 2, 2010.
- DTU Aqua 2<sup>nd</sup> Scientific PhD Seminar at Søminestationen Holbæk, Denmark, May 25-26, 2010.
- The Helsinki Summer School on Mathematical Ecology and Evolution, Finland, August 22-29, 2010.



**7. Research presentations outside DTU  
Mathematics**

*Borghoff, Julia*

- “Bivium as a Mixed-Integer Programming Problem” ISG Seminar, Royal Holloway, University of London. Egham, UK, June 17, 2010.

*Branner, Bodil*

- “Why Mathematics continues to fascinate me – surgery in holomorphic dynamics in particular”, invited talk, at the British Women in Maths Meeting, April 16, 2010, the Isaac Newton Institute, Cambridge, UK.
- “The Structure Theorem of degree  $d$  complex polynomial Vector fields in  $\mathbb{C}$ ”, invited lecture at the 8th AIMS International Conference on Dynamical Systems, Differential Equations and Applications, May 27, 2010, Dresden, Germany.
- “Holomorphic Dynamics I. The dynamical plane”, DMF’s sommertræf for kandidatstuderende i matematik, August 12, 2010, Søminestationen, Holbæk, Denmark.
- “Quasiconformal surgery I and II”, two lectures, September 27, 2010, Workshop on Holomorphic Dynamics around Thurston’s Theorem, RUC, Denmark.
- “The importance of EWM. The EMS committee on Women in Mathematics”, October 6, 2010, at Workshop for Women in Maths in Denmark, Søminestationen, Holbæk, Denmark.
- “Polynomial Vector Fields in one complex variable in  $\mathbb{C}$ ”, invited lecture, at Conformal Dynamics and Hyperbolic Geometry. October 21, 2010, CUNY Graduate Center, New York, US.

*Brander, David*

- “The generalization of Bjoerling’s problem for minimal surfaces to non-minimal CMC surfaces”, ICMS2010, Sharjah, March 2010.
- “Solving geometric Cauchy problems via infinite dimensional techniques”, DGA2010, Brno, Czech Republic, August 2010.

*Brøns, Morten*

- “Dynamical systems and fluid mechanics”, Roskilde University, October 7, 2010.

*Christensen, Ole*

- A survey on duality in frame theory. San Francisco State University, USA January 19, 2010

- On the duality principle. NUS Singapore, March 31, 2010.
- May 30, 1995 – the day Pete entered frame theory. Maryland University, USA, May 22, 2010.
- Frames and unbounded operators. Acoustic Research Institute, June 15, 2010.
- Frames und duality. TU Munich, Germany, July 10, 2010.
- An introduction to frames and the duality principle. Xiamen University, August 17, 2010.

*Gauravaram, Praveen*

- École normale supérieure (ENS), Paris, France during the visit in April and May 2010. Title of the talk: Indifferentiable compression functions
- Microsoft Research India (MSR). Bangalore, India during the visit between 25<sup>th</sup> November and 3<sup>rd</sup> December. Title of the talk: Improved Security Analysis of Fugue-256 hash function and its weaker version.

*Hansen, Vagn Lundsgaard*

- Invited lecture “Good conduct in the sciences” for the IMM Graduate School ITMAN as an ITMAN Research Seminar, DTU, May 10, 2010.
- Invited lecture “Keeping Mathematical Awareness Alive” at the workshop “Raising the Public Awareness of Mathematics”, Óbidos, Portugal, September 26-29, 2010.

*Hjorth, Poul G.*

- Lecture: “Study Groups in Denmark - A Tale of Two Cities”, University of Warwick, UK, March 8, 2010.

*Høholdt, Tom*

- “Decoding of Reed-Solomon Codes”. Lecture at Sabancı University, Turkey, June 1, 2010.

*Knudsen, Kim.*

- “Mathematical aspects of Inverse Problems”, Lectures at ESGI PhD course at DTU, August 13, 2010.

*Schilder, Frank*

- “Continuation of sets of constrained orbit segments”, Department of Mathematics, University of Surrey, UK, Februar 26, 2010.
- “Continuation guided experiments” and “Stabilisation of vortices in the wake of a circular cylinder”, WIAS Berlin, Germany, December 16, 2010

### *Schmidt, Karsten*

- Seminar at LearningLab DTU, November 16, 2010. Presentation: “Web-based Teaching in introductory mathematics at DTU.”
- Seminar at ESTEEM, University of Aarhus December 10, 2010. Presentation: “Web-based Teaching in introductory mathematics at DTU.”

### *Starke, Jens*

- “Nonlinear Dynamics in Science and Engineering”, Nagoya University, Japan, February 19, 2010.
- “Nonlinear Dynamics in Science and Engineering”, TOYOTA CRDL, Nagakute, Japan, February 22, 2010.
- “Equation-free analysis of traveling waves in microscopic traffic models”, Tokyo Metropolitan University, Japan, April 7, 2010.
- “Deterministic and stochastic modelling of catalytic surface processes”, University of Tokyo, Japan, April 22, 2010.
- “Analysis of traveling waves in traffic models”, University of Stuttgart, Germany, July 8, 2010.
- “Mathematical Modelling and Analysis of Complex Nonlinear Processes in the Olfactory System”, Humboldt University Berlin, Germany, December 6, 2010.

### *Stolpe, Mathias*

- “Solving Optimal Design Problems by an Interior Point Method”, TUDelft, the Netherlands, March 2, 2010.
- “Structural Topology Optimization from a Mathematical Programming Perspective - Challenges and Topics for Collaboration”, TUDelft, the Netherlands, October 25, 2010.

### *Thomassen, Carsten*

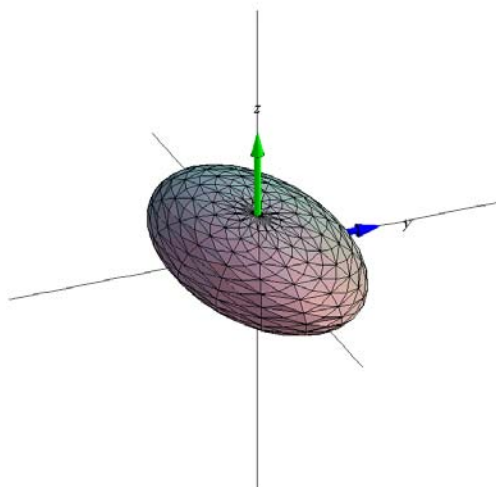
- Rendez-vous numbers and von Neumann’s min-max theorem in game theory”, Colloquium at KAIST, South Korea, April 1, 2010.
- On the Number of Spanning Trees, Orientations, and Cycles, Lecture at KAIST, South Korea, April 2 2010.
- Graphs and maps on surfaces, One hour lecture at C&O Summer school, University of Waterloo, Canada July 5, 2010.
- Electrical networks and random walks, One hour lecture at C&O Summer school, University of Waterloo, Canada, July 6, 2010.
- Rendez-vous numbers and von Neumann’s min-max theorem. Keynote lecture at the 17th annual Canadian undergraduate mathematics

conference, University of Waterloo, Canada, July 6-10, 2010.

- Graphs and maps on surfaces, NBIA Colloquium at the Niels Bohr Institute, Copenhagen, October 29, 2010.

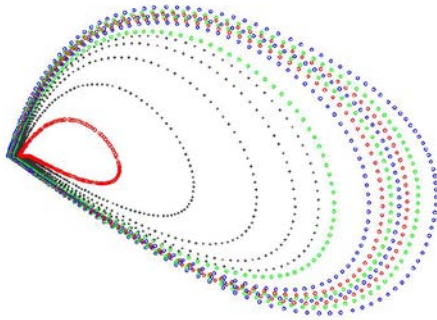
## 8. Teaching activities

For a list of courses in the DTU course catalogue, see <http://www.kurser.dtu.dk>.



### 8.1 Bachelor projects

- Henrik Garde: Wavelets and curvelets. Advisor: Ole Christensen.
- Jacob Larsen, Jonathan Brene: Frames and coding. Advisors: Ole Christensen and Tom Høholdt.
- Tanja Søndergård: Self-dual error-correcting codes. Advisor: Tom Hoholdt.
- Nonlinear pattern formation in the blood coagulation cascade, Kristian Rye Jensen. Advisor: Mads Peter Sørensen.
- The Ginzburg-Landau equations and fluxons in type II superconductors. Rho Malik
- Loving. Advisors: Mads Peter Sørensen and Niels Falsig Pedersen.
- Jens Christian Hillerup: Cryptanalysis of Rejsekortet. Advisor: Erik Zenner.
- Philippe Jørgensen: Linear and Differential Cryptanalysis of the Present light-weight cipher. Advisor: Erik Zenner.



### 8.2 Master projects

- Magnus Plesner: List decoding of Reed-Solomon codes. Advisor: Tom Høholdt.
- Johan S.R. Nielsen, List decoding of error-correcting codes. Advisor: Tom Høholdt.
- Sofie Moth: Sigma-Delta quantization. Advisor: Ole Christensen.
- Jens Broberg: Cache-Timing Attack in 2010. Advisor: Erik Zenner. Co-Advisor: Sven Karlsson (DTU Informatics).
- Michael Dreyer Kollemorten (032061):
- Cryptographic hash functions. Advisors: Lars R. Knudsen, Søren S. Thomsen, Praveen Gauravaram.
- Mathematical modelling of the blood coagulation cascade. Julie Refsgaard Lawaetz.
- Advisors: Mads Peter Sørensen and Nina Marianne Andersen.
- Martin Mehl Lauridsen. "Integer Factorization". Advisors: Lars R. Knudsen, Søren S. Thomsen.
- Krzysztof Slowinski: Cryptanalysis of the Skein hash function. Advisors: Lars R. Knudsen, Krystian Matusiewicz, Søren S. Thomsen.

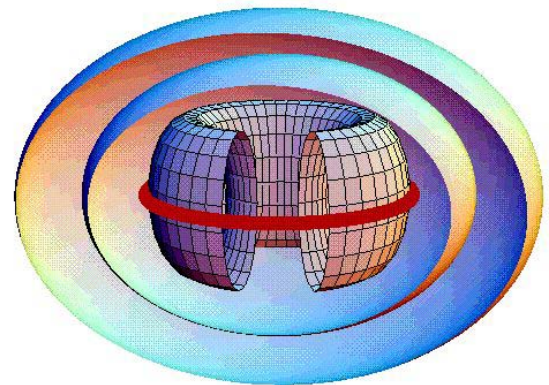
### 8.3 One-off courses at DTU (Specialkurser)

- Classification of polynomial vectorfields in the plane. Two students, Advisor: Christian Henriksen.
- Riemannian Geometry, 1 student. Advisors: David Brander and Steen Markvorsen.
- ECMI Modelling Week Wroclaw, 2010. 2 students. Advisor: Ove Skovgaard.
- Introduction to the Mathematics of Topology Optimization, 1 student, Advisor: Mathias Stolpe
- Functional Analysis – Honors version, 1 student. Advisor Mathias Stolpe.

- 01650 Superconducting wind turbines - hands on, 8 students. Advisor: Mads Peter Sørensen, Asger Bech Abrahamsen, Risø-DTU, Jørn Bindslev Hansen, DTU Physics, Bogi Bech Jensen, DTU Electro.
- Cryptanalysis and cryptographic keys. 1 student. Advisor Erik Zenner.

### 8.4 Continuing education

- Starke, Jens: "A Short Course in Nonlinear Dynamics", 3 days, Toyota CRDL, Nagakute, Japan, February 23-25, 2010.
- Starke, Jens: "Biomathematics in the olfactory system: From receptor neuron dynamics over axonal pathfinding and sorting to spatio-temporal activities in the bulb", 4 hours course, Dansk Matematisk Forening, DMF-sommertræf, Sømimestationen Holbæk, August 12, 2010.
- Starke, Jens; Organizer of international bachelor summerschool "Mathematical Modelling, Nonlinear Dynamics, Stochastic and Complex Systems", together with L.E. Christiansen, P. Hjorth, J.B. Jørgensen, H. Madsen, F. Schilder, M.P. Sørensen, Technical University of Denmark, 59 international participants, August 22-28, 2010.



### 8.5 Other teaching activities

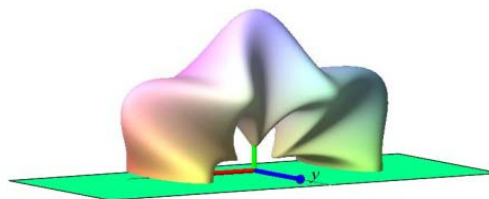
- Participation in joint bi-weekly seminar between RUC and DTU on Holomorphic Dynamics, two semesters in 2010. Branner, Bodil; Henriksen, Christian.
- Lecture, "An Introduction to Denmark and DTU" for KAIST students, February 23 and October 14, 2010, Ole Christensen.

## Annual Report 2010 – Department of Mathematics DTU

- Author of 01426 Cryptology 2 Course offered in semester 2, Praveen Gauravaram.
- Fagpakkeprojekt. Conformal mappings of the tetrahedron, 2 students. Advisor: Christian Henriksen.
- Member of the ECMI Educational Committee, Ove Skovgaard.
- Member of ECMI evaluation panel at the ECMI Modelling Week, Milan, Italy, September 9-12, 2010, Ove Skovgaard.
- Member of DTU CampusNet Committee, Ove Skovgaard.
- Member of DTU G Databar Committee, Ove Skovgaard.
- Vagn Lundsgaard Hansen gave the lecture “Om matematikkens to ansigter” at the summer school “DMF’s sommertræf” for master students in mathematics at the Danish universities, arranged by the Danish Mathematical Society at Søminestationen in Holbæk, August 11-14, 2010 .
- Poul G. Hjorth has supervised one Master student at University of Copenhagen.
- Director of studies for the bachelor study programme Mathematics and Technology, Peter Røgen.
- Major revision of the bachelor education, Mathematics and technology, Peter Røgen.
- Fagpakkeprojekt: Gabor frames. Advisor Ole Christensen
- One-day lecture on continuation using the continuation package COCO as part of a workshop on continuation software held at the University of Bristol, UK, October 11-12, Frank Schilder.
- Kim Knudsen is main advisor for Lai Zhang. Co-advisor: Ken Haste Andersen and Uffe Høgsbro Thygesen, DTU-Aqua.
- Lars R. Knudsen is main advisor for Julia Borghoff.
- Lars R. Knudsen and Gregor Leander are advisors for Valerie Gauthier Umana.
- Lars R. Knudsen is advisor for Mohamed Abdelraheem; co-advisor is Erik Zenner.
- Erik Zenner is co-advisor for Naveed Ahmed (DTU Informatics).
- Mathias Stolpe is main advisor for Eduardo Munoz. Co-advisors: Erik Lund, Department of Mechanical Engineering, Aalborg University.
- Mathias Stolpe is main advisor for Oded Amir. Co-advisor: Ole Sigmund, DTU Mechanical Engineering.
- Mathias Stolpe is main advisor for Marie-Louise Højlund Rasmussen. Co-advisors: Anton Evgrafov DTU Mathematics and Ole Sigmund, DTU Mechanical Engineering.
- Mathias Stolpe is co-advisor for José Blasques, DTU Mechanical Engineering. Main advisor: Christian Berggren, DTU Mechanical Engineering.
- Mathias Stolpe is main advisor for Alemseged Gebrehiwot Weldeyesus. Co-advisor is Erik Lund, Department of Mechanical Engineering, Aalborg University.
- Jens Gravesen is main advisor for Peter Nørtoft Nielsen. Niels Leergaard Pedersen, DTU Mechanical Engineering, is co-advisor.
- Jens Gravesen is main advisor for Dang Manh Nguyen. Anton Evgrafov is co-advisor.
- Mads P. Sørensen is main advisor for Victor Manuel Rodríguez Zermeño.
- Mads P. Sørensen is main advisor for Nina Marianne Andersen.
- Mads Peter Sørensen is co-advisor for Anna Gordeeva, DTU Physics. Main advisor Jesper Mygind.
- Carsten Thomassen is external advisor for two visiting Iranian Ph.D. students.

### 8.6 Advising of PhD. students

- Peter Beelen is main advisor for Johan Sebastian Rosenkilde Nielsen, Tom Høholdt is co-advisor.
- Jens Starke is main advisor for Michael Elmegård. Co-advisors: Jon Juel Thomsen (DTU Mechanics) and Anton Evgrafov.
- Bodil Branner is co-advisor for Steffen Junge. Main advisor is Kari Hag, the Norwegian University of Science and Technology (NTNU) in Trondheim.
- Poul G. Hjorth has supervised Marie Bro Dunn.
- Poul Hjorth is main Ph.D. advisor for Louis Pedersen. Co-advisor: Kim Knudsen.
- Morten Brøns is main advisor for Johan Rønby Pedersen. Co-advisor: Hassan Aref, Fluid DTU and Virginia Tech.



## 9. Research related tasks

### 9.1 Participation in committees of national and international research foundations, international research societies, and private foundations

#### Branner, Bodil

- Member of the Scientific Advisory Board of Centre de Recerca Matemàtica (CRM), Barcelona.
- Member of the committee *Women in Mathematics* under the auspices of European Mathematical Society (EMS).

#### Brøns, Morten

- Member of the National Committee for Theoretical and Applied Mechanics.
- Member of the National Committee for Mathematics.
- Member of the Scientific Council of DCAMM.
- Member of the DCAMM Annual Speaker Committee.

#### Christensen, Ole

- Member of DCAMM Scientific Council.

#### Gauravaram, Praveen

- Member of International Association of Cryptologic Research (IACR).
- Member of DCAMM.

#### Hansen, Vagn Lundsgaard

- President of “The Danish Academy of Natural Sciences”.
- Member of “European Academy of Sciences (Brussels)”.
- President of “The Danish Mathematical Society”.
- Member of the Danish National Committee for Mathematics Education (ICMI-Denmark).

#### Hjorth, Poul G.

- Secretary of the Danish Mathematical Society.

#### Høholdt, Tom

- Member of Wissenschaftliche Beirat, Institut für Experimentelle Mathematik, Essen, Germany.

#### Knudsen, Lars R

- Chairman of the executive committee for Fast Software Encryption series of annual workshops.

#### Starke, Jens

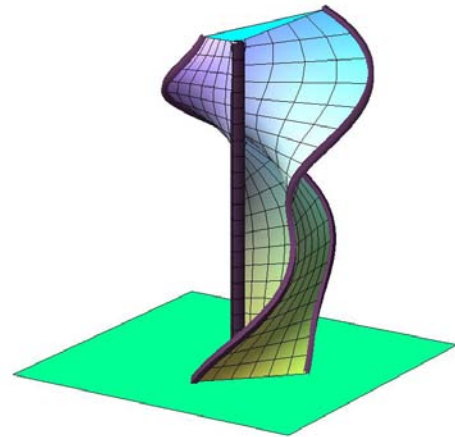
- Member of the Advisory Board, Dynamics Days Europe.
- Member of the Robotics Task Force of IEEE/CIS.

#### Sørensen Mads Peter.

- Member of the ECMI Council. (European Consortium for Mathematics in Industry).
- Member of the OECD Global Science Forum Experts Group on Mathematics in Industry.

#### Thomassen, Carsten

- Member of the Royal Danish Academy of Sciences and Letters.
- Founding Fellow and Member of Board of the Institute of Combinatorics and its Applications (Winnipeg, Canada).



### 9.2 Editorial work for international journals

#### Branner, Bodil

- Associate editor of *Qualitative Theory of Dynamical Systems*.

#### Brøns, Morten

- Editor of *Proceedings of the Third International Symposium on Bifurcations and Instabilities in Fluid Dynamics, 2010*.
- Editor, *ISRN Mechanical Engineering*.

#### Christensen, Ole

- Editor for *Sampling Theory in Signal and Image Processing*.
- Editor for *Asian-European Journal of Mathematics*.

## Annual Report 2010 – Department of Mathematics DTU

- Editor for Journal of Wavelets.
- Editor for J. Indian Society of Industrial and Applied Mathematics.
- Editor for Annals of Functional Analysis.

*Hansen, Vagn Lundsgaard*

- Editor "Nordisk Matematisk Tidsskrift" (Normat).
- Fagredaktør "Aktuel Naturvidenskab".

*Hjorth, Poul G.*

- Editor for "MICS: Mathematics in Industry Case Studies" (Fields Institute, Toronto).

*Høholdt, Tom*

- Editorial Board: Advances in Mathematics of Communication

*Knudsen, Lars R.*

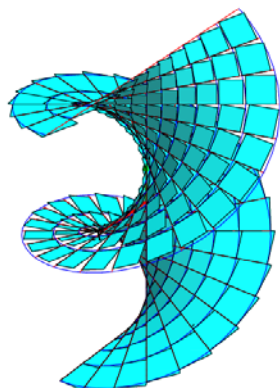
- Associate editor, Journal of Cryptology
- Associate editor, IEEE Transactions on Information Forensics and Security.

*Pedersen, Michael*

- Editor, Biophysical Reviews and Letters
- Editor, Journal of Biomathematics and Biostatistics.

*Thomassen, Carsten*

- Editor in chief, Journal of Graph Theory.
- Editor in chief, Electronic Journal of Combinatorics.
- Editor, Journal of Combinatorial Theory, Ser. B.
- Editor, Combinatorica
- Editor, European Journal of Combinatorics
- Editor, Discrete Mathematics
- Editor, The Australian Journal of Combinatorics



### 9.3 Review work for international journals

*Beelen, Peter*

- 9 articles reviewed for several scientific journals.

*Branner, Bodil*

- Proc. Amer. Math. Soc. (1)

*Brander, David*

- Journal of the London Mathematical Society (1)
- Bulletin of the London Mathematical Society (1)
- Math. Reviews (2)
- Zentralblatt (6)

*Brøns, Morten*

- SIAM Journal on Applied Mathematics (1)
- Journal of Fluid Mechanics (1)
- Journal of Visualization (2)
- SIAM Journal on Dynamical Systems (1)
- Physics of Fluids (1)
- Journal of Fluids and Structures (1)

*Christensen, Ole*

- Appl. Comp. Harm Anal. (3)
- J. Functional Analysis (1)
- J. Math. Anal. Appl. (1)
- Math. Reviews (3)
- Indian J. Pure Appl. Math. (1)
- Expositione Math. (1)
- Current trends in wavelets (1)
- Asian-European J. Math. (1)
- M. Funct. Anal. Top. (1)
- Lin. Alg. Appl. (2)
- Bull. Iran. Math. Soc. (1)
- Banach Journal of Math. Anal (1)
- ISRN Math. Anal. (1)
- IEEE Trans. Inf. Theory (1)
- Tamkang J. Math. (1)
- Mediterranee J. Math. (1)
- Int. J. Of Mathematics (1)

*Gravesen, Jens*

- Computer Aided Geometric Design
- Computer Aided Design

*Gauravaram, Praveen*

- Design, Codes and Cryptography (1).
- IET Information Security (1).
- Transactions on Information Forensics & Security (1).
- IEICE Transactions (1).

## Annual Report 2010 – Department of Mathematics DTU

- 17th International Workshop on Fast Software Encryption (FSE 2010) (1).
- 16th Annual International Conference on the Theory and Application of Cryptology (Asiacrypt 2009) (2).
- Eurocrypt 2010, 29th International Cryptology Conference. (2).
- 17th Annual International Conference on the Theory and Application of Cryptology (Asiacrypt 2009) (3).
- 11th International Conference on Cryptology in India (Indocrypt 2010) (8). Also a programme committee member for this conference.
- 12th International Conference on Information and Communication Security Conference (ICICS 2010) (6). Also a programme committee member for this conference.

### *Hansen, Vagn Lundsgaard*

- Mathematical Reviews (3).
- Zentralblatt für Mathematik (5).
- European Journal of Engineering Education (9).

### *Hjorth, Poul G.*

- 3 papers (only 1 entry) for Journal of Physics A: Mathematics and General.

### *Høholdt, Tom*

- IEEE-Transactions on Information Theory (6)
- ISITA 2010 (3)
- ITW2010 (3)
- YACC 2010 (3)
- Information Processing Letters (2)
- International Journal of Information and Coding Theory (2)
- EURASIP Journal of Advances in Signal Processing (2)

### *Knudsen, Kim.*

- Physiological Measurements
- Inverse Problems
- Journal of Mathematical Analysis and Applications

### *Knudsen, Lars R.*

- Various journals

### *Schilder, Frank*

- AMS Reviews (5).
- Foundations of Computational Mathematics.
- Journal of Physics A: Mathematical and Theoretical.

### *Skovgaard, Ove*

- Ocean Engineering (1 article).

### *Starke, Jens*

- Physics Letters A (1 article).
- Nonlinear Dynamics (1 article).
- IEEE Symposium Series in Computational Intelligence 2011 (3 articles).

### *Stolpe, Mathias*

- Structural and Multidisciplinary Optimization (5 articles)
- Engineering Optimization (1 article)
- Optimization and Engineering (1 article)
- Computational Optimization and Applications (1 article)
- TOPR (1 article)

### *Sørensen, Mads Peter*

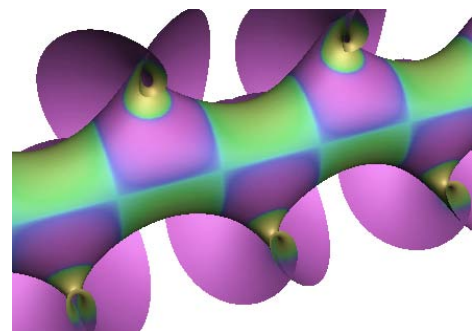
- Mathematics and Computers in Simulation
- Nonlinear Analysis Series A: Methods and Applications
- Physical Review A
- Physical Review B
- Physical Review E
- Mechanics Research Communications

### *Thomassen, Carsten*

- Referee in 2010 for Discrete Mathematics (1 paper)
- Referee in 2010 for Combinatorica (1 paper)
- Referee in 2010 for Graphs and Combinatorics (1 paper)
- Advice in 2010 on a paper for Annals of Mathematics

### *Zenner, Erik*

- Cryptography and Communications (1)
- International Journal of Network Security (1)



### 9.4 Evaluations

#### *Brøns, Morten*

- Evaluation of a proposal for Israel Science Foundation, 2010.
- Evaluation committee for PhD student Teis Schnipper, Department of Physics, December 2010.
- Evaluation committee for a Doctoral Thesis submitted to DTU. 2010.
- Evaluation report for a promotion to Associate Professor at Michigan Technological University, USA.

#### *Christensen, Ole*

- Evaluation of book proposal, Birkhäuser (2).
- Evaluation of PhD thesis, NUS Singapore.
- Evaluation of PhD thesis + role as opponent, Lappeenranta Univ. of Technology, Finland.
- Evaluation of application, Austrian Science Foundation.
- Evaluation of proposal, Graduate Women in Science.
- Evaluation of application, Portuguese Foundation for Science and Technology.
- Evaluation (chairman), position as Associate Professor, DTU Mathematics.

#### *Gauravaram, Praveen*

- Evaluation of Master's Thesis, August 31, 2010. Michael Dreier Kollemorten (032061): Cryptographic hash functions. Evaluated together with Lars R. Knudsen, Søren S. Thomsen and Carsten Dahl Frehr (IBM).

#### *Hansen, Vagn Lundsgaard*

- Evaluation of the Draft Framework for the Assessment of Mathematics in PISA 2012. Comments submitted to Achieve, Washington, U.S.A., August 22, 2010.
- Chairman of the PhD committee for Ojaswa Sharma at DTU Informatics. Defence September 10, 2010.

#### *Høholdt, Tom*

- Member of Committee, Ph.D. Aarhus University.
- Member of Committee, Full professor, University of Urbana-Champaign, Illinois, USA.
- Member of committee, Full Professor, State University of San Diego, USA.
- Evaluation of book proposal, Birkhäuser, 2010.

#### *Knudsen, Kim*

- Member of the PhD committee for Pedro Caro, Universidad Autonoma de Madrid, Spain, June 2010.

#### *Knudsen, Lars R.*

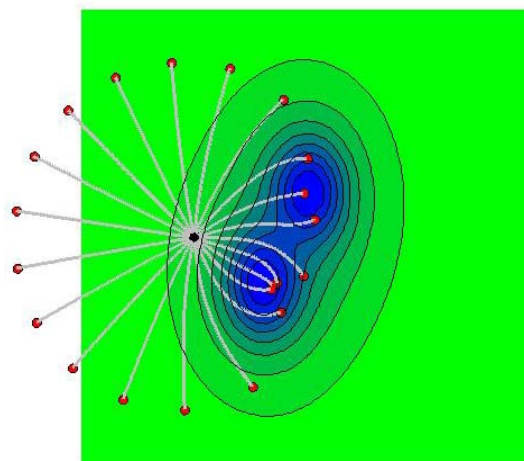
- Member of the PhD committee for Tor E. Bjørstad, University of Bergen, Norway, March 2010.
- Member of the PhD committee for Muhammad Reza Z'Abu, Queensland University of Technology, Australia, Spring 2010.

#### *Sørensen, Mads Peter*

- Member of the Ph.D. committee for Peter Larsen, DTU Physics, and Oscar Andrés Prado Rubio, Department of Chemical and Biochemical Engineering, DTU.

#### *Thomassen, Carsten*

- Carsten Thomassen evaluated in 2010 a proposal for election of a fellow of the Royal Society, England.
- Carsten Thomassen was in 2010 a member of the selection committee for an associate professor position at The University of Southern Denmark.
- Carsten Thomassen evaluated in 2010 an application for Habilitation (right to become Professor) at Université Bordeaux 1, France.
- Carsten Thomassen evaluated in 2010 an application for a position as Professor at University of Birmingham, England.



## 10. Popularizing Science

### 10.1 "Ny viden": Presentations for high-school students

#### Branner, Bodil

- "Kaos og fraktaler i dynamiske systemer", high school students at UNF Matematik Camp, July 14, 2010, Copenhagen University, Denmark.

#### Brøns, Morten

- Simple, complicated and chaotic dynamics. "New Science" lecture held for high school classes from Viborg, Nørresundby, Ordrup and TEC Lyngby
- Dynamics and numbers. Lecture held for UNF, January 2010.

#### Christensen, Ole

- "New Science" lectures (1)

#### Hansen, Vagn Lundsgaard

- "Den geometriske omverden", Gruppe af naturfagslærere fra Bergen, Norge, March 19, 2010.
- "Den geometriske omverden", Viborg Gymnasium og HF, October 12, 2010.
- "Den geometriske omverden", Teknisk Gymnasium (HTX) Esbjerg, October 27, 2010 (in Esbjerg).
- "Ikke-euklidisk geometri", Sct. Knuds Gymnasium, Odense, November 4, 2010. "Den geometriske omverden", Sct. Knuds Gymnasium, Odense, November 4, 2010.

#### Hjorth, Poul G.

- Poul G. Hjorth has given 4 lectures in the lecture series 'The World in a Natural Science Perspective' at the Open University ('Folkeuniversitetet') in Copenhagen, October-December 2010.

#### Markvorsen, Steen

"Hvorfor og Hvordan Krummer Rummet?":

- Odder Gymnasium, 19 students, 3.g. January 28, 2010.
- Ringerike Gymnasium, Norway, 28 students. April 23, 2010.
- Sct. Knuds Gymnasium, Odense, 11 students, 3.g. November 5, 2010.

#### Markvorsen, Steen

"Boomerang! Geometrisk Form og Funktion i Aktion"

- Helsingør Gymnasium, 8 students, 3.g. May 5, 2010.
- Ordrup Gymnasium, 22 students, 3.g. December 1, 2010.

#### Markvorsen, Steen

"Euler's Elastiske kurver"

- Kolding Gymnasium, 35 students, 3.g. November 3, 2010.

#### Starke, Jens

- "Control of distributed robots based on Darwin's selection principle: survival of the fittest", talent camp for school children in Nordsjælland, Denmark, Januar 19, 2010.

#### Sørensen, Mads Peter

- Kaos teori og orden. Foredrag i Ungdommens Naturvidenskabelige Forening, DTU, September 16, 2010.

#### Thomassen, Carsten

- Carsten Thomassen gave the lecture "Graphs and Networks" at the Gymnasium TEC Lyngby, on April 28, 2010.
- Carsten Thomassen gave the lecture "Graphs and Networks" for high school students at Lemvig Gymnasium, on September 28, 2010.
- Carsten Thomassen gave the lecture "Graphs and Networks" in Ungdommens Naturvidenskabelige Forening on October 12, 2010

#### Thomsen, Søren Steffen

"Enigma - en krypteringsmaskine"

- Fysiklærerdag. 2 short lectures on Enigma. March 9, 2010.
- Aurehøj Gymnasium, 60 students. March 17, 2010.
- 40 year anniversary, class of 1970. Presentation of the Enigma. May 20, 2010.
- Viborg Katedralskole, 24 students. September 30, 2010.
- Gladsaxe Gymnasium, 30 students. September 30, 2010.
- Tørring Gymnasium, 21 students. October 1, 2010.
- Maribo Gymnasium, 26 students. October 29, 2010.
- Tradium (Randers Tekniske Gymnasium), 30 students. December 2, 2010.
- HerlufsholmSkole, 25 students. December 7, 2010.

#### Zenner, Erik

- 2 lectures in the lecture series 'The World in a Natural Science Perspective' at the Open Uni-

versity ('Folkeuniversitetet') in Copenhagen, September 2010.

### 10.2 Other activities in popularizing science

*Hansen, Vagn Lundsgaard*

- Four lectures at the Open University (Folkeuniversitetet) in the series "The World in a Scientific Perspective; The Mathematical Foundations", autumn, 2010.
- Gave the lecture "Hvordan skelner man mellem akademisk skidt og kanel?" ("What is wrong and what is right in academics?") in "Akademiet for Talentfulde Unge" ("Academy of Talented Youth"), March 6, 2010.
- Gave the lecture "Matematiske dimensioner" ("Mathematical dimensions") in 'Ungdommens Naturvidenskabelige Forening', UNF-Aalborg, March 9, 2010.
- Gave the lecture "Rundt om Uendeligheden" at a meeting in SeMat (Seminariernes Matematiklærerforening) in Odense on August 20, 2010.
- At the occasion of the 25<sup>th</sup> Anniversary of HTX in Esbjerg, Vagn Lundsgaard Hansen gave the lecture "Matematik i dagligdagen" ("Mathematics in daily life") at an arrangement open to the general public on October 27, 2010.

*Knudsen, Kim.*

- "Pagerank og lineær algebra", Masterclass for High School teachers, Sorø November 4, 2010.

*Markvorsen, Steen*

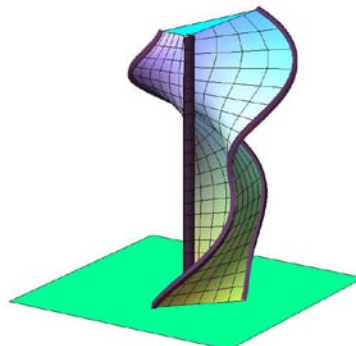
- The experimental talk and presentation. "Boomerang! Geometric Form and Function in Action" has been given in connection with:
  - a) The yearly high school physics teachers day at DTU (organized with Nanoteket DTU Physics, att. O. Trinhammer) on March 9, 2010.
  - b) The 40 years and 60+ years alumne celebrations on May 20 and June 10, 2010 respectively.
  - c) DTU science day. Visit by 80 K9 students from Rudersdal municipality on October 1, 2010.

*Jens Starke*

- "Teambuilding in Engineering and Science", half day teambuilding event for 30 engineers of Atkins & Grontmij, Carl Bro, Denmark, October 5, 2010.

*Thomsen, Søren Steffen*

- A presentation on cryptology at "Åbent Hus DTU", March 4, 2010.



## 11. Other information

### 11.1. International and national collaboration - management of projects etc.

*Christensen, Ole*

- Coordinator for the student exchange program DTU – KAIST.
- Dual degree and research programs DTU-KAIST.

*Gravesen, Jens*

- Member of the steering group for NANO-DTU.

*Høholdt, Tom*

- Manager of the FNU- project: Algebraic Coding Theory 2008-2011.

*Skovgaard, Ove*

- Erasmus/Socrates coordinator for a number of European Universities.

*Starke, Jens*

- Head of project "Equation-free analysis of mechanical vibrations" funded by the Danish Research Council FTP, 2009-2012.

*Stolpe, Mathias*

- Member of the Technical Steering Committee in the Danish Centre for Composite Structures and Materials (DCCSM) 2010- 2017. The partners in the centre include Risø DTU (Materials Research Division & Wind Energy Division), DTU Mechanical Engineering, Department of Mechanical Engineering at Aalborg University, DTU Civil Engineering,

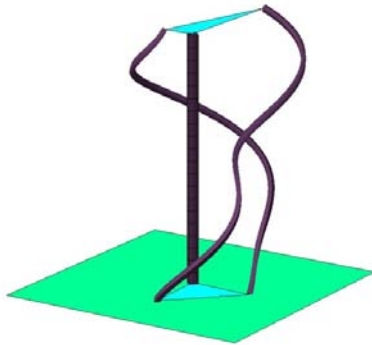
DTU Nanotech, DTU Mathematics, Siemens Wind Power, LM Glasfiber, Fiberline Composites, Bach Composite Industry. The centre homepage is [www.dccsm.dk](http://www.dccsm.dk).

*Sørensen, Mads Peter*

- European Consortium for Mathematics in Industry (ECMI). Council member. Managing the DTU Mathematics computer facilities. Implementation of Danish standard DS 484. Member of the steering groups of the projects: FlowHEAD and NAMEC.

*Thomassen, Carsten*

- Carsten Thomassen was in 2010 principal investigator of the FNU research grant “Research activities in Discrete Mathematics”.



**11.2 Organization of international conferences etc.**

*Brøns, Morten*

- Member of the Scientific Committee for 4<sup>th</sup> International Symposium on Instabilities and Bifurcations in Fluid Dynamics, Barcelona, Spain, 2011.

*Gauravaram, Praveen*

- Programme Committee Member for the 12th International Conference on Information and Communication Security Conference (ICICS 2010).
- Programme Committee Member for the 11th International Conference on Cryptology in India (Indocrypt 2010).

*Henriksen, Christian*

- Co-organizer of workshop and Ph.D. course: “Around Thurston’s Theorem”, Sømimestationen Holbæk, September 27- October 1, 2010.

*Hjorth, Poul G.*

- Organized the 76th European Study Group with Industry, DTU, Kgs. Lyngby, Denmark, August 16-20, 2010 (with J. Gravesen).

*Høholdt, Tom*

- Member of Scientific Committee ITW 2010.
- Member of Scientific Committee ISITA 2010.

*Knudsen, Lars R.*

- Programme committee member of Eurocrypt 2010.

*Starke, Jens*

- Organizer of Brain modes 2010 at DTU: Noise, oscillations and frequency locking in neural systems, together with A. Daffertshofer} (VU University Amsterdam), M. Breakspear (University of New South Wales, Sydney, Australia) and P. Ritter (Bernstein Center for Computational Neuroscience, Berlin & Charite Berlin), <http://www.brainmodes.org>.

*Mathias Stolpe*

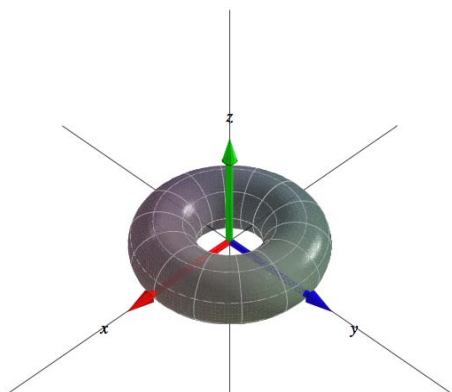
- Organizer (with Erik Lund) of the mini-symposium “Recent advances in structural optimization – modeling and methods”, IV European Congress on Computational Mechanics (ECCM IV): Solids, Structures and Coupled Problems in Engineering, Paris, France, May16-21, 2010.

*Thomassen, Carsten*

- Carsten Thomassen was in 2010 a member of the program committee of the 8th French Combinatorial Conference at Orsay, Paris, FRANCE from June 28 to July 2, 2010.
- Carsten Thomassen is in 2010 a member of the organizing committee of the Canadian Discrete and Algorithmic Mathematics conference (CanaDAM) at the University of Victoria, May 31-June 3, 2011.
- Carsten Thomassen is in 2010 a member of the program committee of the EUROCOMB meeting which will be held in Budapest, Hungary, from August 29, 2011 to September 2, 2011.

*Zenner, Erik*

- Member of program committee for Inscrypt 2010.



### 11.3 Miscellaneous

#### *Brøns, Morten*

- Member of the national committee for written examination in mathematics in the Technical High School (Opgavekommissionen i matematik for HTX).
- Chairman of the board of Trørødkollegiet

#### *Christensen, Ole*

- Talk on International Collaboration, given at meeting with delegation from Vietnam.

#### *Gauravaram, Praveen*

- Young Elite Researcher's Award from the Danish Council for Independent Research, Danish Agency for Science, Technology and Innovation, Ministry of Science, Technology and Innovation, EliteForsk-konference, Ny Carlsberg Glyptotek, Copenhagen, Denmark, January 2010.

#### *Umaña, Valérie Gauthier*

- Visit to INRIA Paris- Rocquencourt, SE-CRET from September 1, 2010 to November 30, 2010.

#### *Hansen, Vagn Lundsgaard*

- Member of Governing Board of 'Folkeuniversitetet i København'.
- Member of Advisory Committee for 'Videnskabs-pædagogiske Aktivitetscentre' representing the Ministry of Science Technology and Innovation. The committee is an inter-ministerial committee appointed by five ministries.
- President of the Jury for Young Scientists in Denmark (Unge Forskere).

#### *Henriksen, Christian*

- Member of group that administrates the MMC Master.

#### *Hjorth, Poul G.*

- Editor of the Danish Mathematical Society Newsletter "Matilde".
- Awarded "DTU Teaching Award 2010".

#### *Høholdt, Tom*

- Member of the Ph.D.-committee for Mathematics, Physics and Informatics.

#### *Markvorsen, Steen*

- Member of the board of Gammel Hellerup Gymnasium, appointed by DTU.
- Consultant conc. patent, co. NVB International. December, 2010.
- Member of the RPA committee (Raising Public Awareness of Mathematics) appointed by EMS, the European Mathematical Society.

#### *Røgen, Peter*

- Member of the board of "Dansk Matematikundervisningskommission", appointed by International Commission on Mathematical Instruction. Until December, 2010
- Chairman for IDA Matematisk Netværk under Danish Society of Engineers, IDA.
- Director of studies for the bachelor education Mathematics and technology.
- Major revision of the bachelor education Mathematics and technology.

#### *Starke, Jens*

- Jens Starke visited the Department of Mathematics, University of Tokyo, Japan from February to May 2010.

#### *Thomassen, Carsten*

- Carsten Thomassen was recommended for (but not awarded) the prize for "Teacher of the year 2010" for his course 01227 Graph Theory.
- The special issue 20 (vol 310, 2010) of the international mathematical journal Discrete Mathematics was dedicated to Carsten Thomassen on his 60th birthday (which was in 2008).

#### *Zenner, Erik*

- Editor of ISO/IEC 18033-4, Amendment 1 (Stream Ciphers).

