department NEWS

Interdisciplinary Biosciences in the Department

Faculty in the department are engaged in highly interdisciplinary research involving collaborations with experimental scientists from the College of Medicine, College of Engineering and Applied Science, and the Department of Biology. Applications range from population genetics to blood flow to biofilms in urban water pipes. The mathematical techniques used in these investigations involve ordinary and partial differential equation models, scientific computation and perturbation methods.

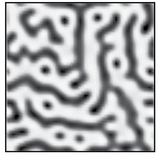
The biomathematics group consists of Professors Sookkyung Lim, Donald French, Steve Pelikan and newcomer Benjamin Vaughan. Lim uses scientific computation to study aortic aneurysms and has used a technique called the immersed boundary method to model the movement of flagella which propel bacteria such as *E. Coli*. French has ongoing collaborations with neuroscientists in the College of Medicine; he is building a computational model of the synchronized bursting in networks of cultured cortical neurons with Eric Gruenstein, and is also investigating ion channel distributions in olfactory cilia with Steve Kleene. Pelikan works on the genetics and geometry (spatial structure) of small populations and estimating the origins of hybrids in collaboration with Steve Rogstadt from biology. He has also done research in bioinformatics. Vaughan, whose work is described elsewhere in this issue, developed numerical methods (the extended finite element method or XFEM) for moving interfaces and boundary layer problems, which were applied to study the growth of and signaling in bacterial biofilms. He has also examined spontaneous pattern generation (morphogenesis) as well as mathematical models of fluids in pulmonary systems.

The group has already had several PhD students (Jiyeon Oh, Dorjsuren Badamdorj and Zeynep Teymuroglu). French and Lim are now collaborating with Nick Cogan from Florida State and Margaret Kupferle in civil engineering on models of biofilm growth in drinking water pipes. Cogan was the Visiting Scholar for the Taft Research Seminar series last fall on Mathematical Modeling of Biofilms.

Benjamin Vaughan Joins Department's Biomathematics Research Group

Benjamin Vaughan

The department welcomes new assistant professor Benjamin Vaughan. Vaughan comes to us after a year-long postdoctoral position at the University of Michigan in the Biomedical Engineering Department, where he helped develop mathematical and numerical models of fluid delivery in the lungs of premature infants. When premature infants are born they may be unable to produce the necessary pulmonary surfactants, which can cause Infant Respiratory Distress Syndrome (IRDS). The normal treatment is to instill liquid surfactants to the lungs, and this kind of research is working to help physicians better understand surfactant distribution and improve patient care.



A modeled pattern of Amazon catfish skin.

Prior to this, Vaughan completed a two-year postdoctoral position at the Centre for Mathematical Biology at University of Oxford where his research focused on spontaneous pattern generation (morphogenesis) in embryonic fish, birds and mammals. Improving upon existing models, Vaughan and his collaborators were able to study these patterns through multi-scale non-linear analysis and numerical simulations, which demonstrated that these models could be used to explain the spontaneous pattern formation on the skin of various animals.

Vaughan received his PhD from Northwestern University in Applied Mathematics in 2007 where he developed numerical methods for moving interfaces and boundary layer problems, which were applied to the growth of and signaling in bacterial biofilms. Bacterial biofilms are found frequently in nature in common places such as water pipes, on teeth (as dental plaque), or on scar tissue, which can lead to severe complications in patients with cystic fibrosis. One particularly important aspect studied was quorum sensing, the mechanism through which bacteria signal their presence to other bacteria within their own and other colonies. The virulence of some bacteria increases when the bacterial population reaches a certain threshold and understanding the quorum sensing mechanism could aid in reducing damage done to neighboring tissue.

Current research interests include mathematical biology and physiology, numerical methods for moving interfaces, the finite element method, bifurcation analysis, Turning models, asymptotic analysis, fluid dynamics and transport, lubrication theory, biofluids and biomechanics.

student NEWS

PhD Student Aims to Revolutionize Cryptanalysis

Daniel Cabarcas, a 2009-2010 Taft Graduate Dissertation Fellow, was recently named a Distinguished Dissertation Fellow by the Graduate School for his project, "Mutant Domestication, a Revolution in Polynomial Solving and Cryptanalysis." A native of Colombia, Daniel came to UC to study computer science. Computer science and cryptography are closely allied and Cabarcas began participating in a joint cryptography seminar run by Jintai Ding and Dieter Schmidt. As a result of this seminar, he joined the PhD program in mathematics to work with Ding. This article is based on his description of his research project.

Cabarcas (above) and his advisor Jintai Ding worked with colleagues in Germany to introduce the world's fastest and most memory-efficient polynomial solvers, called MXL3 and MGB.

The ideal of internet freedom depends on information security. Piracy, electronic theft and espionage pose challenges beyond national boundaries and governments. In response, the use of encryption has become ubiquitous: not only in the government and military, but also in civilian infrastructure such as flash drives, mobile phones and ATM machines. The security of modern encryption systems lies in the extreme difficulty of discovering the secret key. Now, the security of today's society is being jeopardized by a new generation of information attacks on encryption systems known as algebraic attacks. Even the current U.S. encryption standard AES (Advanced Encryption Standard), which is widely used by the government and commercial users and expected to become a global standard, may be in danger of an algebraic attack. It is paramount for the stability of our civilization to investigate the scope of these attacks.

The problem of finding the secret key can be translated into the problem of finding an efficient method for solving a system of polynomial equations, and algebraic geometry tools are now being exploited to enhance this process. The equations involved are nonlinear, and the process of solving them involves introducing additional auxiliary equations (a process called "enlargement") to produce a system that can be solved. By studying the complexity of solving systems of polynomial equations, safe security levels can be established.

Recently Cabarcas and his advisor Jintai Ding worked with colleagues in Germany to introduce the world's fastest and most memory-efficient polynomial solvers, called MXL3 and MGB. MGB (Mutant Gröbner Basis Algorithm) is the first solver ever to solve 32 random equations in 32 variables. The speed-up in the time to solve polynomials was possible thanks to the concept of mutant polynomial that was introduced in 2007 by Ding. "Mutants" are certain polynomials of a lower degree than expected that appear in the process of solving a system of polynomial equations. Mutant polynomials are the core of a long-term ongoing project that involves research groups at UC, the Technical University of Darmstadt in Germany and at Academia Sinica in Taiwan. The realization of their existence allowed Ding, Cabarcas and their collaborators not only to exploit them in accelerating the process, but also to enhance understanding of the complexity of the process. Additional speed was obtained through the use of "flexible partial enlargements." These results cause the researchers to conjecture that there are flaws in current security levels of cryptosystems.

Cabarcas' goal is to establish more precise security estimates using an approach he likes to call Mutant Domestication. While previous work has focused on exploiting the appearance of mutants in a heuristic way, he is progressing in explaining the process of mutant formation. The domestication of mutants will allow him to estimate more precisely the complexity of solving systems of polynomial equations, thus produce accurate security levels for algebraic attacks. He predicts that mutant domestication will yield faster solvers, as the understanding of the nature of mutants will allow the manufacture mutant polynomials at will.

alumni NEWS

Wesley Darbro (BS, '65), an aerospace engineer at NASA for the last 42 years, writes, "My office blackboard is covered with discussion on finite geometries, dual nature of points and lines, various proofs of sizes of infinity, because of Gaylord Merriman and David Lipsich. I was a fellow student with David Minda and Jim Deddens. Fond memories." Darbro enclosed a poem he published in the April 1972 issue of Physics Today that includes the lines

But others stand, straight and tall
With emotion they behold
What makes the heart beat hard and fast
And can't be bought with gold.
They've sat transformed in a master's class,
Merriman, Lipsich and many more.
The master's light that burned so bright
In them is all aglow.

Tina Hunter

Tina Hunter (MS, '03; PhD, '08) has been hired as Senior Director of Analytics for S2 Statistical Solutions, Inc., a leading provider of data mining and economic analysis for medical device, diagnostic and biopharmaceutical companies. In this newly created position, Hunter will be managing the growing statistical effort at S2 as the company continues to expand its data analysis and research offerings. Previously, Hunter was a biostatistician with StatKing Consulting, Inc., where she provided statistical support to sponsors of clinical trials for medical devices, pharmaceuticals and diagnostics. In this position, she wrote statistical analysis plans, interim analysis plans, and the statistical sections for protocols and clinical study reports. In addition, she represented companies in negotiations with the Food and Drug Administration (FDA). Prior to StatKing, Hunter performed exploratory data analysis and statistical modeling activities for the U.S. Environmental Protection Agency. Hunter was a student of Siva Sivaganesan.

Shuang Kang (PhD, '10), a recent PhD in financial mathematics (advisor: Srdjan Stojanovic) accepted a position with the quantitative analytics arm of Fitch Solutions, a division of the Fitch Group. The quantitative analytics team conducts academic-quality research on a broad range of quantitative finance modeling, including credit risk, interest rate risk and market risk. The group features researchers located in London and New York who cover a wide range of specialties including: data manipulation and statistics, empirical credit risk modeling, arbitrage free valuation and hedging, cash flow analysis, advanced econometrics, applied mathematics, simulation techniques, derivatives, as well as hands-on structured finance and banking experience.

Robert B. Koch (BS, '50) passed away on Aug. 12, 2009 after some years of cardiac troubles and serious heart surgery on August 10th. He retired in 1986 from the John Hancock Life Insurance Co. after working as vice president group insurance actuary since 1960, and enjoyed his retirement years in Albuquerque, N.M.

Tell us what you think!

McMicken College strives to keep math alumni informed of the latest news in the department. Please take a few minutes to tell us what you think about this newsletter in our on-line survey at: ***www.surveymonkey.com/s/artsci_newsletters***
Your feedback is invaluable and will help us better serve the needs of alumni by providing the news you care about and enjoy reading most.

Sign up for McMicken Monthly

Have all the latest news from McMicken College delivered straight to your inbox once a month. Sign up today for the McMicken Monthly e-newsletter at ***www.artsci.uc.edu/mcmickenmonthly***.

What's new with you?

Please use the enclosed form to include your latest news in the next issue of The Right Angle and other McMicken College publications. You can also submit your news online at: ***www.artsci.uc.edu/updates***.

THE RIGHT ANGLE

THE RIGHT ANGLE is produced by the Department of Mathematical Sciences McMicken College of Arts and Sciences University of Cincinnati PO Box 210025 Cincinnati, OH 45221-0025

Editor: Joanna Mitro
For more information, call (513) 556-4050 or e-mail us at RightAngle@math.uc.edu
Comments and suggestions are welcome.

Layout and design by McMicken College of Arts and Sciences Office of Marketing and Communications

Please affix postage here

THE RIGHT ANGLE
Department of Mathematical Sciences
McMicken College of Arts and Sciences
University of Cincinnati
PO BOX 210025
Cincinnati, OH 45221-0025

F O L D H E R E

from the EDITOR

We welcome your comments and suggestions, and encourage you to keep in touch with us. Please use this form, e-mail us at *RightAngle@math.uc.edu*, or share your news with any faculty member who was important to you. Faculty e-mail addresses can be found at www.math.uc.edu.

Joanna Mitro

Name _____
Address _____
_____
Year of graduation _____
Degree _____
Current occupation _____
Professional or personal news (comments/suggestions):
_____
_____
_____
_____
_____
_____

THE RIGHT ANGLE
Department of Mathematical Sciences
McMicken College of Arts and Sciences
University of Cincinnati
PO Box 210025
Cincinnati, OH 45221-0025

RETURN ADDRESS REQUESTED

Non-profit
Organization
U.S. Postage
PAID
Permit No. 133
Cincinnati, OH

the HYPOTENEWS

Jintai Ding

Jintai Ding was the winner of UC's 2010 Sigma Xi Young Faculty Research Award. This award recognizes distinguished scientific research accomplishments by faculty members within 15 years of their terminal degree. In connection with the award, Ding presented the lecture "Does IT Really Make The World More Secure?: Security in the Ubiquitous Computing World and the Importance of Multivariate Public Key Cryptography" during Undergraduate Research Poster Week in June.

Magda Peligrad

Also in June, **Magda Peligrad's** seminal work in probability theory was the focus of a conference in her honor held in Paris, France. The conference, titled "Limit Theorems for Dependent Data and Applications" featured 24 distinguished speakers, including several of Peligrad's co-authors. The author of over 68 papers and book chapters, she is a Distinguished Taft Research Professor and an associate editor for the Journal of Mathematical Analysis and Applications. Her research is currently supported by grants from the National Security Agency.

THE RIGHT ANGLE

McMicken
College of Arts & Sciences

Vol. 18, Mathematics Alumni Newsletter, Autumn 2010
Department of Mathematical Sciences
RightAngle@math.uc.edu

UNIVERSITY OF Cincinnati

from the HEAD

Shuang Zhang

As the new department head, I would like to warmly greet you all from the Department of Mathematical Sciences. Under the nine-year leadership of Tim Hodges, the department has improved significantly in research, teaching and service. I express sincere appreciation for Tim's dedicated service.

Since last fall the department has been busy on two key issues: preparing for semester conversion in 2012, and merging the mathematics faculty of the College of Applied Sciences and Center for Access and Transition into the department. The combined department includes different talents in research, instruction and community engagement. I believe that our integrated force will become a highly productive team.

Under the unprecedented economic storm, inadequate resource has squeezed the department to admit fewer master and PhD students. It has become essential to effectively utilize the limited resources and capture new opportunities. We will maintain and later recover the graduate programs, but currently expand the undergraduate program by restructuring the tracks in applied math—in particular, actuarial sciences—that are in high demand both domestically and internationally.

I have already initiated possible joint 2+2 and 2+2+1 programs with Chinese universities. These will create a significant source of revenue and I expect that the restructure will lead to growth of the undergraduate program.

As always, we love to hear from you. You are most welcome to drop us a few lines, suggesting, criticizing and sharing.

Wishing you the best,

Shuang Zhang
Professor and Head
shuang.zhang@uc.edu
513-556-4052

tim hodge's headship COMES TO A CLOSE

Tim Hodges

After nine years as department head, I'm delighted to be able to pass on the reins of the department to Shuang Zhang. I am confident that Shuang will guide the department through the many challenges facing us in the next few years and lead us into a new era of excellence in research and teaching.

My first year as department head began with floods in the department due to some problems with the re-roofing of the building. The last year began with the news that the north wall was gradually pulling away from the rest of the building. At this point, it became clear that someone was trying to tell me something and it might be time to step down! The last nine years have seen enormous changes in the department, the university and the new University System of Ohio. The USO's vision is for a more organized system of universities in which UC's role is that of a major research university. As such we now have a more focused mission than in the past. The main campus will now focus almost exclusively on research, graduate education and four-year undergraduate degrees, with developmental education and two-year degrees passing to the branch campuses and to Cincinnati State. The restructuring associated with these changes first dismantled our University College and replaced it with the Center for Access and Transition which handled developmental education. Last year the CAT was itself dismantled with the developmental duties passing partly to A&S and partly to the branch campuses. The College of Applied Science has been integrated with the College of Engineering and many of the mathematics faculty from both CAS and CAT have joined our department.

In conjunction with these changes, our priorities over the last five years have been development of our research programs, growth of the PhD program and expansion of our external funding. We have been extremely successful in all three directions, hiring some excellent young researchers with international reputations; increasing our PhD graduation rates from one to two per year to five or six per year; and just this year achieving record levels of external funding.

The challenging economic climate has seen increased interest in career-based tracks in mathematics and statistics. We have responded by creating an MS in statistics, a five-year joint BA/MS program and a track in actuarial science.

While endowments across the country are shrinking, our department's has actually increased significantly, thanks to an extremely generous gift from the late professor Maita Levine which will provide scholarship funds for women choosing to study mathematical sciences.

It's been a pleasure and a privilege serving as department head over the last nine years, but I'm excited to be returning to a faculty role and my two greatest loves: teaching and research.

Tim Hodges
Professor

Thanks to All of Our 2009-10 Donors

We thank the following individuals and foundations for their generous donations to the department. These gifts fund scholarships, attract and retain the finest faculty, and enrich the experience of our graduate and undergraduate students.

For information on making a gift to the University of Cincinnati, please contact:

Deborah Livingston
513-556-5806
livingdh@ucmail.uc.edu

Dr. Naomi Barnett and Mr. Harvey Gittler
Mr. Robert D. Bergstein
Ms. Nancy L. Diemler
Lawrence and Susan Gilligan
Gilmar Publishing Company
Timothy J. Hodges, PhD
Estate of Maita F. Levine
Mrs. Joanne D. Madison
Carl D. Minda, PhD
Mr. Hollis D. Mitchell
Dr. Joanna B. Mitro
Dr. James M. Osterburg
Drs. Costel and Magda Peligrad
Raymond H. Rolwing, PhD
Tara L. Smith
Francis B. Thomas, PhD
Mr. James M. Thompson
Paul R. Wilson, PhD