

# MAT 332 — A journey into geometric complexity: from biological viruses to quantum computing

27 February 2006 — 3 March 2006

Old Main 403 Canisius College: 5:00 — 8:00pm Daily

**Instructor:** Meera Sitharam  
Associate Professor  
CISE Department<sup>1</sup>  
CSE Building  
University of Florida  
Gainesville, FL 32611-6120  
sitharam@cise.ufl.edu  
<http://www.cise.ufl.edu/~sitharam>

## COURSE ABSTRACT:

The primary goals of the course are to expose students to complexity theory through geometric problems; and to the process of extracting and formalizing geometric problems occurring in the real world. The secondary goal is to show how these geometric complexity problems both open up new areas of mathematics as well as provide fresh insights into classical areas.

The course will consist of the following topics, each requiring about 1 hour. Note that the topics could be interspersed. Course material and exercises will be provided on site and key unsolved research problems will be delineated. The primary emphasis will be on:

- (a) motivational, geometric, usually computational problems occurring in real world scenarios,
- (b) on examples to build intuition in order to understand the elegance, depth and richness of these problems, and
- (c) the important process of finding effective formalizations for them. We will only briefly touch upon
- (d) their independent mathematical interest and relevant available classical and modern mathematical techniques for approaching them.

## Geometric complexity of 2 and 3 dimensional structures

- (1) Motivation 1: Geometric constraints in Virus and other Macromolecular Self-organization
- (2) Motivation 2: Geometric constraints in Mechanical Computer Aided Design
- (3) Rigidity characterizations and distance geometry
- (4) Solution spaces and underlying algebraic geometry, tensegrity, unfolding linkages
- (5) Polyhedral constructions, the role of symmetry
- (6) The Game of geometric self-organization: robustness, complexity lower bounds and evolution

---

<sup>1</sup>Computer and Information Sciences and Engineering

## Higher dimensional geometric complexity: embeddings and dimension reduction

- (1) Motivation 1: Mutually unbiased basis (MUB) problem in quantum cryptography
- (2) Motivation 2: approximation of hard optimization problems, learning, codes, pseudorandom generation
- (3) Dimension reduction: impossibility and complexity lower bounds
- (4) The role of symmetry in dimension reduction

### Prerequisites:

- *Minimally*; a good background in calculus together with some exposure to linear algebra and/or discrete mathematics.

### BIOGRAPHICAL INFORMATION:

Meera Sitharam has a Ph.D. in Computer Science from the University of Madison-Wisconsin (1990), with a minor in Mathematics. Sitharam was a Humbolt Fellow at the University of Bonn (1990-91) in Germany, and joined the faculty of the Department of Mathematics and Computer Science at Kent State University in 1992. Sitharam has had visiting positions at Purdue University (1997-98), and the Center for Discrete Mathematics and Theoretical Computer Science (DIMACS) at Rutgers University (Spring 1998). Sitharam is currently a tenured associate professor in the CISE Department at the University of Florida, Gainesville.

Meera Sitharam's research ranges over a variety of topics. She collaborates with mathematicians, theoretical physicists, structural biologists, mechanical engineers and economists. Philosophically, however, her sphere of interests is held together by a common, well-defined thread: accurately defining and capturing the elusive notion of complexity. Within this sphere, she enjoys finding interdisciplinary problems that give rise to rich new mathematical directions or to fresh insight into classical directions. Mathematically, she has noticed that she gravitates to an elegant doorway at the confluence of (asymptotic) geometry, algebra and combinatorics. Sitharam publishes research articles in the topics that currently intrigue her, her M.S. and Ph.D. students and collaborators. Sitharam has directed a number of Research Experiences for Undergraduates, and is currently sponsored by grants from the National Science Foundation.

# MAT 333 — Number Theory, Pseudorandomness and Cryptography

6 — 10 March 2006

Old Main 403 Canisius College: 5:00 — 8:00pm Daily

**Instructor:** Willem Fouché  
Professor  
Department of Decision Sciences  
University of South Africa (UNISA)  
Pretoria, RSA

## COURSE ABSTRACT:

The application of ideas from number theory to the theory of error-correction codes, cryptography and the design of efficient algorithms which are based on discrete patterns which are “pseudorandom”, rank among the deepest aspects of the information sciences. The efficient simulation of randomness have incredibly interesting applications, not only to the design of information systems but also to the understanding of the intrinsic time complexity of algorithms. On the other hand, the security of information systems are frequently brought about by the apparent algorithmic time complexity of some elementary arithmetical processes. The underlying mathematics is very deep and makes substantial use, among other things, of the validity of the *Riemann hypothesis* over finite fields. However, the results are very accessible (in the sense of being easily understood) and it is possible to see the power of these results for information processing even at a relatively elementary level. And, so, this will be the aim of these lectures: To discuss and analyze a number of interesting applications of number theory to information processing.

**Lecture Breakdown:** Five lectures of length three hours each, covering the following topics, in summary.

### Lecture One:

- Basic graph theoretic terminology
- Expander graphs and their applications to coding theory and complexity

### Lecture Two:

- Basic number theory: Euclidean algorithm, modular arithmetic, prime number theorem
- Structure of units modulo prime powers, primitive roots
- Cayley graphs of cyclic groups
- Pseudorandomness

### Lecture Three:

- Euler’s function, Mobius inversion
- Quadratic reciprocity law, computation of Jacobi symbols
- Random constructions: Paradoxical tournaments, graphs with large girth
- Explicit constructions based on quadratic residues modulo primes

**Lecture Four:**

- Probabilistic algorithms: Monte Carlo versus Las Vegas
- Efficient computation of Jacobi symbols
- Principles underlying the random generation of prime numbers
- Applications to public key cryptography

**Lecture Five:**

- Discrete Fourier transforms
- The Weil estimate for trigonometric sums
- Applications of efficient prime number generation to public key cryptography
- Design of independent pseudorandom sequences
- Constructions of expander graphs (An overview)

**Prerequisites:**

- *Minimally*; a good background in calculus together with some exposure to linear algebra and/or discrete mathematics.

## BIOGRAPHICAL INFORMATION:

Willem Fouché started off his mathematical career by studying number theory. His interest shifted to the understanding of the complexity theoretic aspects of number theory which culminated in his linking the algorithmic complexity of Diophantine equations with the descriptive complexity of a Brownian motion. In addition, he studied the recursive aspects of Ramsey theory which soon led to an interest in the role of symmetry in Ramsey theory. This turned out to have applications to topological dynamics and the conceptual aspects of pseudorandomness.

Willem Fouché's work has been published in leading journals, such as *Advances in Mathematics*, *Journal of the London Mathematical Society*, *The Journal of Symbolic Logic* and *Journal of Number Theory*. At the moment he is putting the final touches to an invited monograph on the Wiener process for Springer. Among his former PhD students, six are active researchers in mathematics and its applications, including in computer science. The distinguished international gatherings that he has been invited to address include the 1999-2000 winter meeting of the Association for Symbolic Logic in Washington DC (January 2000) and the Prague Midsummer Combinatorial Workshop XII in July 2005. During the World Mathematical Year 2000 Fouché received a gold medal from the South African Mathematical Society (SAMS) for his achievements. He was awarded the Chancellor's Prize for research at the University of South Africa in 2005 where he is currently the researcher holding the highest rating by the National Research Foundation of South Africa.

Willem Fouché's hobbies include music, hiking and the poetry of the I Ching. He has a keen interest in ancient philosophies and how mathematics may be a reflection of human consciousness.

## MAT 334 — Graphics, Modeling and Animation

20 — 24 March 2006

Old Main 403 Canisius College: 5:00 — 8:00pm Daily

**Instructor: Jorg Peters**  
Professor  
CISE Department  
CSE Building  
University of Florida  
Gainesville, FL 32611-6120  
jorg@cise.ufl.edu  
<http://www.cise.ufl.edu/~jorg>

### COURSE ABSTRACT:

What gives Pixar's characters their looks? How does one simulate a flock of birds? The course participants will discover the power and beauty of affine invariant representations of geometry based on barycentric coordinates, the use of control structures and curved geometry via refinement. (To create digital worlds, Computer Graphics borrows tools ranging from algebraic geometry to differential topology.)

Course participants will create and modify shapes to match tasks and look at programs for graphical interaction with geometry using OpenGL, the lingua franca of graphic programming.

### The modules of study include:

- Bézier representations
- B-splines
- Box-splines
- Subdivision curves and surfaces
- Manipulation of large meshes

### Prerequisites:

- *Minimally*; a good background in calculus together with some exposure to linear algebra and/or discrete mathematics.

### BIOGRAPHICAL INFORMATION:

Jorg Peters obtained a Ph.D. in Computer Science from the University of Madison-Wisconsin (1990). He is now Professor for Computer Graphics and Geometric Modeling in the Department of Computer and Information Sciences and Engineering (CISE) at the University of Florida, Gainesville FL. Prior to this, Peters was faculty at Purdue University (1992-98) and the Rensselaer Polytechnic Institute (1991-92) and he was a Post Doctoral Fellow at the IBM, T.J. Watson Research Center (1990-91).

Since 1990, Jorg Peters' SurfLab - <http://www.cise.ufl.edu/research/SurfLab/> - has been continuously funded by the National Science Foundation (NSF), including a prestigious National Young Investigator award. Moreover, SurfLab has mentored a number of students through REU (*Research Experience for Undergraduates*) programs. Some of these students were subsequently placed into renowned graduate programs at elite American universities.

Jorg Peters' areas of research specialization span graphics; geometric modeling; visualization; and scientific computing and he has published in venues stretching from the Siggraph conference to the journal *Constructive Approximation*. His core interest is in devising and characterizing *geometry representations*. Peters' main theoretical contributions are to the theories of Geometric Continuity and of Subdivision Surfaces and, most recently, to the constructive characterization of one-sided approximation (so as for a smooth path to stay to one side of an obstacle). Peters has designed a number of algorithms, including *N-patches* put into hardware by ATi, a leading supplier of graphics cards, and *surface splines*, used e.g. by Sim-surgery, a Norwegian company pioneering haptic feedback surgery simulation for medical training. One of his recent projects is to create a 3D haptic authoring environment for surgeons.