# WiMSoCal Symposium

## $4^{th}$ Annual Women in Mathematics in Southern California Symposium

**January 21, 2012**
**Loyola Marymount University**

**Titles and Abstracts**

---

Keynote Address by


KRISTIN LAUTER
MICROSOFT, SAN DIEGO


*Elliptic Curve Cryptography & Applications*

---

ABOUT THE SPEAKER: Kristin Lauter is an American mathematician and cryptographer whose research interest is broadly in application of number theory and algebraic geometry in cryptography. She is particularly known for her work in the area of elliptic curve cryptography. She is currently a researcher and the head of the Cryptography Group at Microsoft Research in Redmond, Washington. Lauter received her Bachelor of Arts, Master of Science, and Ph.D., all in mathematics, from the University of Chicago, in 1990, 1991, and 1996, respectively. Prior to joining Microsoft, she held positions as a visiting scholar at Max Planck Institut für Mathematik in Bonn, Germany (1997), T.H. Hildebrandt research assistant professor at the University of Michigan (1996 – 1999), and a visiting researcher at Institut de Mathematiques Luminy in France (1999). In 2008, Lauter, together with her coauthors, was awarded the Selfridge Prize in Computational Number Theory.

**Gulhan Bourget, CSU Fullerton**
*Missing Data in Transmission Disequilibrium Test with One Sib*

The Transmission Disequilibrium Test (TDT) compares frequencies of transmission of two alleles from heterozygous parents to an affected offspring. This test requires all genotypes to be known from parents and an offspring. However, parental or offspring genotypes can be missing. For example, for late onset diseases parental genotypes can be missing. In literature, there have been techniques dealing with missing genotypes. In this talk, I propose a new method to impute missing genotypes that considers the Mendel Inheritance Property and takes into account the population frequency of the disease allele and marker allele in the rTDT method proposed by Sebastiani, Abad-Grau, Alpargu and Ramoni. Our test is more robust than rTDT in terms of type I error rate and the power of the test. The simulation study involving different genetic models (dominant, additive, and recessive), and different missing mechanism will be presented to demonstrate the performances of the test.

---

**Maria Isabel Bueno Cachadina, UC Santa Barbara**
*Eigenvectors for some families Fiedler-like linearizations*

The problem of the computation of eigenvalues and eigenvectors of regular matrix polynomials, which is known as the Polynomial Eigenvalue Problem (PEP), has attracted the attention of many researchers in numerical linear algebra. The standard way to numerically solve the PEP for regular polynomials is through the use of linearizations. These are essentially matrix pencils $H(\lambda) = \lambda X + Y$ sharing certain information with the polynomial $P(\lambda)$, in particular, the invariant polynomials, which include the eigenvalues and its associated partial multiplicities. However, the eigenvectors of $H(\lambda)$ and $P(\lambda)$ are not the same. An important question is how to obtain the eigenvectors of $P(\lambda)$ from those of the linearizations. In this talk we present formulas for the left and right eigenvectors of some families of Fiedler-like linearizations of square matrix polynomials; in particular, for the families of Fiedler pencils, generalized Fiedler pencils and Fiedler pencils with repetition. Additionally, we explain how to obtain the eigenvectors of $P(\lambda)$ for those of the linearizations.

---

**Erin Byrne, Harvey Mudd College**
*The Post-fragmentation Density Function for Bacterial Aggregates*

Multicellular communities are a dominant, if not the predominant, form of bacterial growth. Growing affixed to a surface, they are termed biofilms. When growing freely suspended in aqueous environments, they are usually referred to as flocs. Flocculated growth is important in conditions as varied as bloodstream infections (where flocs can be

seen under the microscope) to algal blooms (where they can be seen from low earth orbit). Understanding the distribution of floc sizes in a disperse collection of bacterial colonies is a significant experimental and theoretical challenge. One analytical approach is the application of the Smoluchowski coagulation equations, a group of PDEs that track the evolution of a particle size distribution over time.

The equations are characterized by kernels describing the result of floc collisions as well as hydrodynamic-mediated fragmentation into daughter aggregates. The post-fragmentation probability density of daughter flocs is one of the least well-understood aspects of modeling flocculation. A wide variety of functional forms have been used over the years for describing fragmentation, and few have had experimental data to aid in its construction. In this talk, we discuss the use of 3D positional data of Klebsiella pneumoniae bacterial flocs in suspension, along with the knowledge of hydrodynamic properties of a laminar flow field, to construct a probability density function of floc volumes after a fragmentation event. Computational results are provided which predict that the primary fragmentation mechanism for medium to large flocs is erosion, as opposed to the binary fragmentation mechanism (i.e. a fragmentation that results in two similarly-sized daughter flocs) that has traditionally been assumed.

---

**Lixian Chen, CSU, San Marcos**

*The Lotka-Volterra Predator-Prey Model and Harvesting Strategies*

In this talk, I will first briefly describe the basics of the classical Lotka-Volterra predator-prey model, and then discuss the predator-prey model modified with logistic growth of the prey. I will further introduce the modified predator-prey model with harvesting of the prey. Different types of harvesting will be briefly introduced, and other variations of the predator-prey model will also be discussed briefly, such as a predator-prey system with harvesting of the predator, a predator-prey system with stocking of prey and/or predator, and a system with one predator and two prey. To numerically approximate the solutions of the predator-prey system with different variations, the explicit Runge-Kutta method has been used. In particular, the Runge-Kutta-Fehlberg method with stepwise control and the Dormand-Prince coefficients are used for better approximation. Investigation of the qualitative behavior of the solutions and the stability analysis of the predator-prey model with harvesting of the prey requires techniques commonly used for study of nonlinear ordinary differential equations. Specifically, we vary the harvest rate in the model and study the change of the equilibrium points, the cycle, the yield of a cycle and the average yield. We start with the analysis for the most basic and simple type of system, and extend to the study of other variations of the predator-prey model with harvesting.

---

**Alona Chubatiuk, USC**
*Nonparametric Bayesian Method of Estimating an Unknown Probability Distribution*

The purpose of this talk is to give an understanding of the basic ideas of the Nonparametric Bayesian approach of estimating an unknown probability distribution; and in particular to define the Dirichlet Process.

Suppose we observe a random sample, of $Y_1, Y_2, \ldots, Y_N$ independent but not necessarily identically distributed random variables, $Y_i \in \mathbb{R}^d$, for $i = 1, \ldots, N$. Assume also that the conditional density of $Y_i$ given $\theta_i$ is known and denoted by $p_i(Y_i|\theta_i)$, where the $\theta_i$'s are unobserved random parameters that are independent and identically distributed with common but unknown distribution function $F$. The objective is to estimate $F$ given the data $Y_1, \ldots, Y_N$.

We use a Nonparametric Bayesian Approach to estimate $F$, describe applications to a common benchmark dataset (Galaxy) and compare the results with other approaches.

---

**Yen Duong, UC Santa Barbara**
*An overview of philosophies of math*

This is an introductory talk in the philosophy of mathematics. We'll consider formalism, logicism, and platonism, and more if time permits.

---

**Nadejda Dyakevich, CSU San Bernardino**
*Long Term Behavior of Solutions for Bernoulli Initial Value Problems*

Bernoulli initial value problems are well researched and used extensively to model processes in physics, economics, biology, and other fields. In this presentation, we will first derive exact (equation specific) conditions for unbounded growth in finite time of solutions for Bernoulli problems with constant coefficients. Then we will extend the results to Bernoulli problems with variable coefficients.

---

**Erica Flapan, Pomona College**
*Intrinsic properties of graphs embedded in $R^3$*

Knot theory is the study of the topology of embeddings of simple closed curves in $R^3$. A natural extension of knot theory is the study of the topology of embeddings of graphs in $R^3$. However, in contrast with knots, the structure of a graph can be complex, and this can affect all of its embeddings. If every embedding of a graph has a particular property, then we say that property is intrinsic to the graph. For example, a graph is said to be intrinsically knotted if every embedding of the graph in $R^3$ contains a knot. In this talk we will discuss intrinsic

knotting and other intrinsic properties of graphs.

---

**Allison Gilmore, UCLA**
*An algebraic approach to knot Floer homology*

Knot Floer homology was first introduced by Ozsvath-Szabo and Rasmussen using the same holomorphic disk counting techniques that underlie Heegaard Floer homology. It can be viewed as a lifting of the Alexander polynomial. I will briefly outline an alternate construction of knot Floer homology that is entirely algebraic, and more similar to Khovanov's HOMFLY homology. I will then explore how these different constructions of knot Floer homology can be viewed as lifting different definitions of the Alexander polynomial.

---

**Katja Goldring, Francesca Grogan, UCLA**
*Difference Equations with an Allee Effect and the Periodic Sigmoid Beverton-Holt Equation Revisited*

We will be examining the Sigmoid Beverton-Holt difference equation. It has been shown that when the Beverton-Holt has a $p$-periodically-varying parameter, there exists a $p$-periodic globally asymptotically stable solution $\{x_n\}$. In our paper, we extend this result to include a more general class of Sigmoid Beverton-Holt functions. Furthermore, we consider the case in which the variables of our general class are varied randomly and show that there exists a unique invariant density to which all other densities converge. Lastly, we extend the Beverton-Holt to include a spatial component and show there exists a unique, stable, non-trivial fixed point in this case.

---

**Ellie Grano, UC Santa Barbara**
*Disambiguated Temperley-Lieb Algebra*

The Disambiguated Temperley-Lieb Algebra is a new associative algebra defined using pictures and local relations. I will present my basis for this algebra as a vector space.

---

**Cymra Haskell, USC**
*The Stochastic Beverton-Holt Equation*

In the Beverton-Holt difference equation of population biology with intrinsic growth parameter above its critical value, any initial non-zero population will approach an asymptotically stable fixed point, the carrying capacity of the environment. When this carrying capacity is allowed to vary periodically it is known that there is a globally asymptotically stable periodic solution and the the average of the state

variable along this solution is strictly less than the average of the carrying capacities, i.e. the varying environment has a deleterious effect on the state average. In this work we consider the case of a randomly varying environment and show that there is a unique invariant density to which all other density distributions on the state variable converge. Further, for every initial non-zero state variable and almost all random sequences of carrying capacities, the averages of the state variable along an orbit and the carrying capacities exist and the former is strictly less than the latter.

---

**Kristin Lauter, Microsoft**
*Elliptic Curve Cryptography and Applications*

In the last 25 years, Elliptic Curve Cryptography has become a mainstream primitive for cryptographic protocols and applications. This talk will give a survey of elliptic curve cryptography and its applications, including applications of pairing-based cryptography which are built with elliptic curves. No prior knowledge about elliptic curves is required for this talk. One of the information-theoretic applications I will cover is a solution to prevent pollution attacks in content distribution networks which use network coding to achieve optimal throughput. One solution is based on a pairing-based signature scheme using elliptic curves. I will also discuss some applications to privacy of electronic medical records, and implications for secure and private cloud storage and cloud computing.

---

**Yanping Ma, Loyola Marymount**
*Population Dynamics Study of Heterotypic Cell Aggregations in the Near-wall Region of a Shear Flow*

This work focused on the modeling of polymorphonuclear neutrophils tethering to the vascular endothelial cells, and subsequential tumor cell emboliformation in a shear flow, an important process of tumor cell extravasation from the circulation during metastasis. A population balance model is utilized, which for the first time, to our best knowledge, a multiscale near-wall collision model reconciles the effect of deformation on cell coagulation procedure, and works for general ratios of heterotypic cell.

---

**Sonja Mitchell, UCSB**
*A Type B Version of Thompson's Group F*

We consider Thompson's Group F as generated by "flip-renormalize" actions on the Farey Tesselation of the hyperbolic plane. Using this approach, we define a Type B version of the group, which we call $F_B$. A construction of $F_B$ and preliminary results will be discussed.

---

**Aisha Najera, CGU**
*A cellular automaton model for drug release from a matrix tablet*

We describe a cellular automaton (CA) model for the dissolution and release of a water-soluble drug and an excipient from a matrix of insoluble polymer. One goal is to capture and understand the observed point of inflection in experimental release curves.

---

**Heather Russell, USC**
*A reduced set of moves on a special subset of knot diagrams*

A famous theorem by Reidemeister gives a complete set of moves that can be used to transition between any two diagrams of the same knot. We discuss a set of Reidemeister-type moves on a subcollection of knot diagrams called one-vertex ribbon graphs. This project is joint with the students and professors in the LSU VIGRE knot theory research at LSU in Fall 2009.

---

**Anna Varvak, Soka Univ of America**
*Generalized continued fractions: a new way of seeing the familiar*

Lukasiewicz paths—lattice paths on non-negative integers with up-steps by arbitrary number of units but down-steps of one unit—exhibit clear multi-recursive features, and their generating function can be expressed by a generalized continued fraction. Moveover, Lukasiewicz paths encode various familiar combinatorial objects: permutations, partitions, idempotent functions, and multipermutations. The generating functions of those objects can then be represented as generalized continued fractions, demonstrating their interesting non-obvious recursive features.

---

**Marilyn Vazquez, CSU, Long Beach**
*Vascular Network Extraction of Small Veins on Placental Surfaces*

Current medical interest in the placenta has inspired vascular network extraction on placenta images. The focus of this research is to develop an automated program that detects the small veins in these images. Their small area and the difficulty to see them even with a bare eye present some of the various challenges to extract them. The Frangi Filter, based on eigenvalues of second derivatives, has been shown to be successful in identifying vessels of varying sizes. However, the placenta's rough and irregular surface are also detected as part of the vessels network; therefore; we propose a new filter, which we called Whale, in addition to the Frangi Filter in order to enhance its results. The Whale Filter takes the result of the Frangi Filter, using $\sigma = 2$,

and marks the most linear components and anything connected to it and discards anything else. Since the background noise is not as linear as the vessels and rarely connected to the vessels, this will be able to remove the background noise and keep the vessels intact. The whale filter has been tried on a 181-by-181-pixel placenta patch and on a whole placenta image of dimensions 1042-by-1117 pixels. The returned results will be shown in the presentation.

---

**Shanshan Xu, USC**
*Non-parametric Multivariate Hypothesis Testing*

In this talk, I will introduce two nonparametric multivariate methods for testing the slope of the regression line. Both methods use MCD(Rousseeuw regression estimator) and bootstrap. The first method uses data depth while the second one use Hotelling's $T^2$ test. By justifying the limiting $p$-value, the first method performs well under various forms of departure from the Gaussian distribution, but under homoscedasity, and the other is robust under heteroscedasticity.

---

**Yi Yang, UCLA**
*Binary Matching Pursuit in 1-Bit Compressive Sensing and Matrix Completion*

We propose a robust method with binary matching pursuit which can be used to recover signals from 1-bit measurements and complete a low-rank matrix when only part of its components are given. For 1-bit CS, this method will detect the positions where sign flips happen and recover the signals using "correct" measurements. For matrix completion, it can find the locations of given components where the data is completely corrupted by noise and use the rest data to reconstruct the matrix.