# Abstracts

Talks by professors take place in Room 110. For parallel sessions, talks written in the first line take place in Room 110 and those written in the second line take place in Room 127.

# Tuesday, 21 January

# 9:30-10:30

#### Jian Zhou (Tsinghua University)

Boson-fermion correspondence and Witten-Kontsevich tau-function

#### Keywords:

**Abstract**: Tau-functions and boson-fermion correspondence play important roles in Kyoto school's approach to integrable hierarchies. An amazing conjecture of Witten proved by Kontsevich states that the generating function of intersection numbers on Deligne-Mumford moduli spaces is a tau-function of the KdV hierarchy. In this talk we will explain some recent result on understanding the Witten-Kontsevich tau-function from the point of view of boson-fermion correspondence.

#### 10:40-11:40

# Takashi Sakajo (Kyoto University)

Mathematical theory of potential flows in multiply connected domains

Keywords: Takashi Sakajo

Abstract: We deal with the incompressible and inviscid flows in two-dimensional domains whose velocity field, say u(t, x) = (u(t, x, y), v(t, x, y)) at time t and at the position x = (x, y), is a solution of 2D Euler equations. Suppose further that the vector field is *irrotational*, namely it satisfies  $v_x - u_y = 0$ . Then the velocity field u(t, x) is represented by a holomorphic function F(z) = u - iv, called the *complex velocity*, in which the complex z-plane is identified with the two-dimensional space as  $z \sim x + iy$ . When the complex velocity has the primitive W(z), i.e. W'(z) = F(z), its imaginary part  $\psi = \text{Im}[W(z)]$ , which is known as the *stream function*, gives rise to the Hamiltonian of the velocity field, i.e.  $u = \partial_u \psi$  and  $v = -\partial_x \psi$ .

When these flows are considered in multiply connected domains, there arise many interesting problems. Mathematically, in the construction of the complex velocity in these domains, a transcendental function called the *Schottky-Klein prime function*, which is an extension of the elliptic functions to an *M*-punctured disk, plays an important role. In order to consider the multiply connected domains with arbitrary boundary shapes, one needs to construct conformal mappings between multiply connected domains mathematically as well as computationally. The other problems are a topological classification of structurally stable Hamiltonian vector fields on multiply connected domains, and a description of all possible transitions between them. On the other hand, from the application point of view, the potential flow theory is available to construct mathematical models that contribute to the theoretical understanding of biofluids such as insect flights and schooling of fish as well as environmental flows in rivers and coastal domains.

In the presentation, I will introduce this theory in multiply connected domains and show its recent research developments with many examples.

# 13:40-14:10

# Hansol Hong (Seoul National University)

Localized mirror functors and HMS for  $\mathbb{P}^1_{a,b,c}(HMS = Homological mirror symmetry)$ 

Keywords: Lagrangian Floer theory, matrix factorizations, Homological mirror symmetry

Abstract: We will begin with a brief introduction to the homological mirror symmetry (HMS for short) conjecture. For a Kähler manifold X, HMS predicts that there is a Kähler manifold Y whose "complex geometry" is equivalent to the "symplectic geometry" of X, and vice versa. Symplectic side of HMS is formulated by a certain  $(A_{\infty}$ -)category called the Fukaya category of X, and for the Landau-Ginzburg mirror  $(Y, W : Y \to \mathbb{C})$  of X, the complex counterpart is given by the matrix factorization category of W.

I will next explain the natural construction of mirror functors between these two categories associated with immersed Lagrangians  $\mathbb{L}$  in X. The construction of the functor depends on the Floer theory of this immersed Lagrangian, in particular, the holomorphic discs one of whose boundary condition is  $\mathbb{L}$ .

We finally apply the construction to the orbifold projective lines  $\mathbb{P}^{1}_{a,b,c}$  together with a specific Lagrangian in  $\mathbb{P}^{1}_{a,b,c}$  which generates the Fukaya category. Here,  $\mathbb{P}^{1}_{a,b,c}$  is an orbifold sphere which has three singular points with  $\mathbb{Z}_{a}$ ,  $\mathbb{Z}_{b}$  and  $\mathbb{Z}_{c}$  singularities, respectively. Our goal is to prove HMS for  $\mathbb{P}^{1}_{a,b,c}$  when  $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} \leq 1$ .

# Xumin Gu (Fudan University)

Partial Regularity of Solutions to the Four-Dimensional Navier-Stokes Equations

#### Keywords: 4D Navier-Stokes equations, partial regularity, Campanato's characterization

**Abstract**: In this talk, we consider suitable weak solutions of incompressible Navier-Stokes equations in four spatial dimensions. We prove that the two-dimensional time-space Hausdorff measure of the set of singular points is equal to zero.

We prove our results in three steps. In the first step, we give some estimates of the scaling invariant quantities. In the second step, we establish a weak decay estimate of certain scaling invariant quantities based on the estimate we proved in the first step by using an iteration method. In the last step, we improve the decay estimate by a bootstrap argument, and apply parabolic regularity to get a good estimate of the  $L^{3/2}$ -mean oscillations of u, which yields the Hölder continuity of u according to Campanato's characterization of Hölder continuous functions.

#### 14:20-14:50

#### Maho Yokota (Kyoto University)

Noether problem for some easy groups

Keywords: Noether problem, rationality, Galois theory

**Abstract**: Let K be a field and G a finite group acting on a rational function field  $K(x_g : g \in G)$  by  $x_g \cdot h = x_{gh}$  for any  $g, h \in G$ . Noether problem asks whether the invariant field  $K(G) := K(x_g : g \in G)^G$  is rational over K or not. This problem is simple, however the answer depends greatly on the property of G and K, and known results are far from general answer.

It is known that K(G) is rational over K if G has a faithful representation of at most degree three and K is algebraic closed. I found if the order of G is odd, the assumption about faithful representation can be weakened. Namely, we only need the following assumptions; K is algebraic closed and G has a faithful representation which is the direct sum of representations of at most degree three. In this talk, I talk about introduction to Noether problem at first and about outline of the proof of my theorem.

#### Jaehoon Kang (Seoul National University)

Tangential limits for harmonic functions with respect to  $\phi(\Delta)$ : stable and beyond

**Keywords**: Bernstein function, subordinate Brownian motion, Poisson kernel, harmonic function, tangential limits,  $L^p$ -Hölder space

Abstract: We study the boundary behavior of harmonic functions with respect to the non-local operator. The classical Fatou theorem, which was showed by Fatou in 1906, states that if  $f \in L^p(\mathbb{R}^{d-1})$  for  $p \in [1, \infty]$ , the Poisson integral of f, defined on the upper half space  $\mathbb{R}^d_+$  has a non-tangential limit for almost every boundary point  $\xi \in \mathbb{R}^{d-1}$ . After the classical Fatou theorem, there have been a lot of studies on the boundary behavior of harmonic functions such as, for general operator and general open set, Fatou theorem, relative Fatou theorem (the existence of non-tangential boundary limit of ratio of two harmonic functions) and the existence of tangential limits. In this talk, we discuss tangential limits for regular harmonic functions with respect to the non-local operator  $\phi(\Delta) := -\phi(-\Delta)$  in the  $C^{1,1}$  open set D in  $\mathbb{R}^d$ , where  $\phi$  is the complete Bernstein function and  $d \geq 2$ . For  $p \in (1, \infty]$  and  $\beta > 1/p$ , suppose that the exterior function f is local  $L^p$ -Hölder continuous of order  $\beta$  on  $D^c$ . Then, we obtain that the regular harmonic function  $u_f$  with respect to  $\phi(\Delta)$ , whose value is f on  $D^c$ , has a boundary limit for almost every  $\xi \in \partial D$  through a parabola that depends on  $\phi$  and  $\phi'$ . Our result includes the case  $\phi(\lambda) = \log(1 + \lambda^{\alpha/2})$ . To prove our results, we use both the probabilistic and analytic methods. In particular, the sharp Poisson kernel estimates are essential to our approach.

#### 15:00-15:30

# Tsung-Ju Lee (National Taiwan University)

Weil-Petersson metric on the moduli of Calabi-Yau varieties

#### Keywords: Weil-Petersson metric, Calabi-Yau, Mixed Hodge structures

**Abstract**: The moduli space of Calabi-Yau manifolds, with a fixed polarization, exists due to a famous theorem of E. Viehweg. It's also known that there is a canonical metric on it, which is called the Weil-Petersson metric. It's interesting to know whether the metric is complete or not. It can be shown that the finite distance property somehow reflects the geometry on the central fiber.

In this talk, I will give the precise statement and review the proof of earlier results, due to Chin-Lung Wang, on the completion problem in the one parameter case. Then I will discuss some of my recent progresses on the relevant results which extend this theorem to some cases where the moduli spaces are of higher dimensions.

# Jung-Hyun Bae (Sungkyunkwan University)

Eigenvalue results for nonlinear maximal monotone operators

Keywords: eigenvalue, maximal monotone operator, degree theory

**Abstract**: In this talk, we deal with some eigenvalue results for maximal monotone operators in reflexive Banach spaces. A theory of maximal monotone operators has been developed by many researchers with applications to operator equations and evolution equations. The study on nonlinear eigenvalue problems is mainly based on degree theories for appropriate classes of nonlinear operators and a regularization method by means of the duality operator.

Let X be a real reflexive Banach space with its dual  $X^*$  and let L be a dense subspace of X. Suppose that  $T: D(T) \subset X \to 2^{X^*}$  is a maximal monotone operator and  $C: D(C) \subset X \to X^*$  is a densely defined operator with  $L \subset D(C)$ . We consider an eigenvalue problem of the form

$$0 \in Tx + \lambda Cx.$$

We present some eigenvalue results concerning operators of  $(S_+)$  type, with the aid of a Kartsatos-Quarcoo degree theory.

#### 16:00-16:30

#### Yong Wei (Tsinghua University)

Sharp diameter estimates for compact manifold with boundary

Keywords: Diameter estimate, Manifold with boundary, Ricci curvature, Rigidity

**Abstract**: Let (N, g) be an *n*-dimensional complete Riemannian manifold. The classical Myers' theorem says that if the Ricci curvature of (N, g) has a positive lower bound  $Ric \ge n-1$ , then the diameter of N is at most  $\pi$ . S.-Y. Cheng proved that if the diameter is equal to  $\pi$ , then N is isometric to the *n*-sphere  $\mathbb{S}^n(1)$ .

Recently, M. M. Li generalized the above theorems to manifold with boundary. He showed that if the Ricci curvature of (N, g) is nonnegative and the mean curvature of the boundary  $\partial N$  satisfies  $H \ge (n-1)c_0 > 0$  for some constant  $c_0 > 0$ , then the distance from any interior point x to the boundary  $\partial N$  has an uniform upper bound  $1/c_0$ . Moreover, if  $\partial N$  is compact, then N is also compact. If the distance from some point x to the boundary achieves the maximum  $1/c_0$ , then N is isometric to a ball of radius  $1/c_0$  in an n-dimensional Euclidean space  $\mathbb{R}^n$ .

In the case that the manifold (N, g) has a negative lower bound  $Ric \ge -(n-1)$ , and the mean curvature of the boundary  $\partial N$  satisfies  $H \ge (n-1)c_0 > (n-1)$  for some constant  $c_0 > 1$ , a standard argument can also give the diameter bound

$$\sup_{x \in N} d(x, \partial N) \le \coth^{-1} c_0. \tag{1}$$

If  $\partial N$  is compact, then (1) implies that N is also compact.

In this talk, we show if the equality holds in (1), then N is isometric to a geodesic ball of radius  $\operatorname{coth}^{-1} c_0$  in an *n*-dimensional hyperbolic space  $\mathbb{H}^n(-1)$ .

#### Yuri Yatagawa (The University of Tokyo)

Two invariants of ramification

Keywords: ramification, Swan conductor, Artin conductor, cleanliness

**Abstract**: In this talk, we study one difference between two invariants of ramification, the refined Swan conductor and the refined Artin conductor.

In number theory, these two conductors are defined for the character of a representation of a Galois group over a complete discrete valuation field. We call this representation a Galois representation. A (complete) valuation field is a generalization of an algebraic field or an algebraic function field over a finite field. For an algebraic field (i.e. a finite extension of  $\mathbb{Q}$ ) and the integer ring (i.e. the integral closure of  $\mathbb{Z}$  in the algebraic field), we can consider the problem "how prime ideals of  $\mathbb{Z}$  decompose in the integer ring," and we can also consider for an algebraic function field over a finite field (i.e. a finite extension of k(T) where k is a finite field) and the integral closure of k[T] in the algebraic function field. Ramification means this decomposition in number theory.

In arithmetic geometry, we can treat discrete valuation fields with smooth varieties and divisors of them. And in this case, a character of a Galois representation corresponds to a smooth sheaf over the complement of a divisor. For this sheaf, we can generalize the two conductors above, and these are very important invariants related to a formula of the Euler characteristic of the sheaf. In this talk, we consider a surface, and see one difference between these two conductors with respect to the resolution of bad points.

#### 16:40-17:10

# Zhi-You Chen (National Central University)

On the Uniqueness and Structure of Solutions to the System Arising from Chern-Simons Models

Keywords: Uniqueness, Chern-Simons system

**Abstract**: Firstly, we review some well-known results about the Chern-Simons equation with single Higgs particle:

$$\Delta u + \frac{1}{\varepsilon^2} e^u (1 - e^u) = 4\pi \sum_{i=1}^{N_1} \mu_i \delta_{p_i} \text{ in } \mathbb{R}^2.$$

Secondly, to the Chern-Simons equation with two Higgs particles:

$$\begin{cases} \Delta u + \frac{1}{\varepsilon^2} e^v (1 - e^u) = 4\pi \sum_{i=1}^{N_1} \mu_i \delta_{p_i} \text{ in } \mathbb{R}^2, \\ \Delta v + \frac{1}{\varepsilon^2} e^u (1 - e^v) = 4\pi \sum_{j=1}^{N_2} \nu_j \delta_{q_j} \text{ in } \mathbb{R}^2. \end{cases}$$

we prove the uniqueness of topological multivortex solutions (i.e,  $(u(x), v(x)) \rightarrow (0, 0)$  as  $|x| \rightarrow \infty$ ) if either the Chern-Simons coupling parameter is sufficiently small  $\varepsilon > 0$  or sufficiently large  $\varepsilon > 0$ . In addition, the sharp range of flux for non-topological radial solutions and structure of all entire solutions are also derived.

#### Hirokazu Shinjo (Tohoku University)

Coefficients of L-functions of certain type of curves

Keywords: L-functions, Jacobian variety, GL<sub>2</sub>-type, Formal group, Honda theory

Abstract: For algebraic curve C over  $\mathbb{Q}$ , the L-function of C is important and interesting object in arithmetic geometry. For example, let p be a good prime of C, counting the numbers of rational points on reduction modulo p of C is equivalent to determine the coefficients of polynomial  $L_p$ , the p-component of L. When C is elliptic curve and p is good prime, Manin showed the congruency between the coefficient of  $L_p$  and the Hasse-Witt matrix. Honda showed this more globally by using the strong isomorphism of two formal groups, one is a formal minimal model of C over  $\mathbb{Z}$ , the other is attached to L. I will talk about the generalization of this congruency to curves whose Jacobian variety is  $GL_2$ -type, and some example of calculating the coefficients of  $L_p$ .

# 17:20 - 17:50

# Kotaro Kawai (Tohoku University)

Deformations of associative submanifolds in nearly parallel  $G_2$ -manifolds

**Keywords**: Associative submanifolds,  $G_2$  geometry

**Abstract**: A Riemannian 7-manifold (Y, g) is called a nearly parallel  $G_2$ -manifold if the holonomy group of its cone is contained in Spin(7). An associative submanifold M in Y is defined to be a minimal 3-submanifold which is related to the nearly parallel  $G_2$ -structure of Y.

A typical example of nearly parallel  $G_2$ -manifolds is a 7-sphere  $S^7$ . In this talk, we assume that  $Y = S^7$  for simplicity, and study submanifolds in  $S^7$ . There are various classes of associative submanifolds arising from other geometries. Special Legendrian 3-submanifolds in  $S^7$ , arising from the Calabi-Yau geometry on  $\mathbb{R}^8$ , are associative, and Lagrangian submanifolds in a totally geodesic  $S^6$ , arising from the  $G_2$  geometry on  $\mathbb{R}^7$ , are immersed into  $S^7$  as associative submanifolds.

We study the infinitesimal deformations of associative submanifolds, and compare deformation spaces in these classes. Then we study the homogeneous associative submanifolds in  $S^7$  explicitly.

#### Seongan Lim (Ewha Woman's University)

On the Homomorphic Encryption NTRU

Keywords: Cryptography, public key encryption, homomorphic encryption, NTRU

**Abstract**: An homomorphic encryption scheme allows computing over ciphertexts and it is expected as a very useful cryptographic primitive for secure cloud services. Among many known homomorphic encryption schemes, the homomorphic version of NTRU is the only one which manipulates ciphertexts for different users simultaneously. In this talk, we review the history of several published NTRU-variants and present an algebraic analysis of the parameters for the homomorphic NTRU.

# Wednesday, 22 January

# 9:30-10:30

# Jungkai Chen (National Taiwan University)

Geography of varieties of general type

# Keywords:

**Abstract**: In classification theory of algebraic varieties, we are interesting in the distribution of birational invariants of varieties, such as genus, volume and Euler characteristics. A priori, these invariants could be arbitrarily large. However, they satisfies famous Miyaoka-Yau Inequality and Noether Inequality in dimension 2. In this talk, we will explore the three dimensional analogue of these inequalities.

# 10:40-11:40

#### Quanshui Wu (Fudan University)

Poisson (co)homology and duality

#### Keywords: Poisson algbera; Poisson (co)homology; Poicare duality

Abstract: Poisson algebras play an important role in Poisson geometry, non-commutative geometry and mathematical physics. Poisson homology and Poisson cohomology are important invariants of Poisson structures. The set of Casimir elements of the Poisson structure is the 0-th cohomology; Poisson derivations modulo Hamiltonian derivations is the 1-st cohomology. In the talk, I will start from the basic definitions and examples, such as Poisson algebras, poisson modules, Poisson homology and cohomology. Then I will talk about a (twisted) duality theory between Poisson homology and Poisson cohomology, and prove a version of the twisted Poincare duality between the Poisson homology and cohomology for any polynomial Poisson algebras with values in an arbitrary Poisson module, which generalizes the results in literature. In the case that the Poisson structure is unimodular, the twisted Poincare duality reduces to the Poincare duality in the usual sense.

#### 13:40-14:10

## Koichi Shimada (The University of Tokyo)

Group Actions on von Neumann Algebras

# Keywords: von Neumann algebra, group action

Abstract: In this talk, we will explain a classification of group actions on von Neumann algebras. We consider algebras consisting of linear operators on a Hilbert space. A von Neumann algebra is such an algebra which is closed under a suitable topology. For example, the matrix algebra  $M_n(\mathbb{C})$ , acting on the Hilbert space  $\mathbb{C}^n$ is a von Neumann algebra. Another example is essentially bounded functions  $L^{\infty}(\mathbb{R})$ , acting on the Hilbert space  $L^2(\mathbb{R})$  by multiplication. Although these examples are not so interesting, by doing kinds of manipulations on these examples, many examples of von Neumann algebras are obtained. We are interested in studying properties of these von Neumann algebras. One of the methods to understand these von Neumann algebras is to study their symmetry, that is, to study group actions on von Neumann algebras. The first breakthrough in this area has been done by A. Connes in 1970's. He has classified the integer group actions on a von Neumann algebra constructed by taking an inductive limit of matrix algebras. In this talk, we explain some progress of classification of group actions on von Neumann algebras after Connes. In particular, the real number group actions. Contrary to the integer group, the real number group is not discrete. We will explain the difficult point of the classification of  $\mathbb{R}$ -actions on von Neumann algebras and partial answers for this by many people, including Kawahigashi, Kishimoto, Kawamuro, Masuda–Tomatsu and us.

#### Kameng Nip (Tsinghua University)

#### Combinations of Shop Scheduling and the Shortest Path Problem

**Keywords**: Approximation algorithm, combination of optimization problems, flow shop, open shop, job shop, scheduling, shortest path

**Abstract**: We consider several novel combinatorial optimization problems, which combine the classic shop scheduling problems (namely, flow shop scheduling, open shop scheduling or job shop scheduling) and the

shortest path problem. The objective of the obtained problems is to select a subset of jobs that forms a feasible solution of the shortest path problem, and to execute the selected jobs on the shop (flow shop, open shop or job shop) machines to minimize the makespan. We show that these problems are NP-hard even if the number of machines is two, and cannot be approximated within a factor less than 2 if the number of machines is an input unless P = NP. We design several approximation algorithms for these combination problems.

#### 14:20-14:50

# Ryunosuke Ozawa (Tohoku University)

Limit formulas for metric measure invariants and phase transition property (A joint work with Takashi Shioya (Tohoku University))

**Keywords**: Metric measure space, concentration, observable distance, separation distance, pyramid, phase transition

**Abstract**: We consider Gromov's compactification of the set of metric measure spaces. An element of the compactification is called pyramid. In this talk, we generalize the observable diameter and the separation distance for metric measure spaces to those for pyramids, and study the limit of these invariants for a convergent sequence of pyramids. As an application, we obtain a criterion of the phase transition property for a sequence of metric measure spaces or pyramids, and find some examples of symmetric spaces of noncompact type with the phase transition property. This talk is based on a joint work with Takashi Shioya (Tohoku University).

#### Sheng-Hua Chen (National Taiwan University)

Edge Roman Domination on Graphs (A joint work with Chun-Hung Liu and Gerard Jennhwa Chang)

Keywords: Graph theory, domination theory, discharging method

Abstract: Let G = (V, E) be a simple graph. An edge Roman dominating function on G is a function  $f : E(G) \to \{0, 1, 2\}$  satisfying that every edge  $e_1$  for which  $f(e_1) = 0$  is adjacent to at least one edge  $e_2$  for which  $f(e_2) = 2$ . The weight of a Roman dominating function is the value  $f(E) = \sum_{e \in E(G)} f(e)$ . The minimum weight  $\gamma'_R(G)$  of a edge Roman dominating function on a graph G is called the edge Roman domination number of G. The concept of the edge Roman domination was first introduced in [2].

In this talk, we investigate some upper bounds using discharging method and other skills.

[1] S. Akbari, S. Qajar, On the edge roman domination number of planar graphs, manuscript.

[2] P. Roushini Leely Pushpam, T. N. M. Nalini Mai, Edge Roman domination in graphs, J. Combin. Math. Combin. Comput. 69 (2009), 175–182.

#### 15:00-15:30

# Jiyoung Han (Seoul National University)

Distribution of integral lattice points in an ellipsoid with a diophantine center

Keywords: Equidistribution, lattice point counting and Heisenberg group

Abstract: Using representation theory and symplectic geometry combined with equidistribution theorem on the Jacobi group  $Sp(n, \mathbb{R}) \ltimes \mathbb{R}^{2n}$ , we evaluate the mean square limit of exponential sums related with a rational ellipsoid  $\{a_1x_1^2 + \cdots + a_nx_n^2 = 1\}$ , extending a work of Marklof. The result helps to study the asymptotic values of the normalized evaluations of the number of lattice points inside a rational ellipsoid and inside a rational thin ellipsoid.

# Myeongmin Kang (Seoul National University)

Inexact accelerated augmented Lagrangian method for linearly constrained  $\ell_1$ - $\ell_2$  minimization

**Keywords**: Augmented Lagrangian method, Acceleration, Compressive sensing, inexact solution **Abstract**: We consider the linearly constrained  $\ell_1$ - $\ell_2$  minimization:

$$\min_{x} \|x\|_{1} + \frac{\beta}{2} \|x\|_{2}^{2} \text{ subject to } Ax = b.$$

In compressive sensing, a linearly constrained  $\ell_1$  minimization problem, i.e., the problem (1) with  $\beta = 0$ , where an underdetermined system of equations, has been used. Adding the  $\|\cdot\|_2^2$  in the basis pursuit problem yields the tractable objective function, which is a strictly convex function. Thus, the linearly constrained  $\ell_1 - \ell_2$  minimization problem has a unique solution and the dual problem is smooth. We apply augmented Lagrangian method to the linearly constrained  $\ell_1 - \ell_2$  minimization. But, the augmented Lagrangian method has the subproblem and does not have the closed form solution. In this talk, we propose an inexact accelerated augmented Lagrangian method for solving this minimization problem. In our algorithm, we give the stopping conditions of subproblem. The proposed method is based on the extrapolation technique, which is used in accelerated proximal gradient methods proposed by Nesterov. A convergence rate of  $\mathcal{O}(\frac{1}{k^2})$  is proved for the proposed method when it is applied to solve a more general linearly constrained nonsmooth convex minimization problem. We numerically test our proposed method on a synthetic problem from compressive sensing. The numerical results confirm that our inexact accelerated augmented Lagrangian method is faster than state-of-arts algorithms.

#### 16:00-16:30

# Li Ming (Fudan University)

The interior estimate for convex solutions of k-Hessian equations and a rigidity theorem

#### Keywords: interior estimate, k-Hessian equations, Dirichlet problem

**Abstract**: The interior  $C^2$  estimates for Monge-Ampére equations were studied firstly by A.V. Pogorelov. Then K.S Chou and X-J. Wang extended Pogorelov 's estimates to the case of k-Hessian equations. Explicitly, in their paper, for any function f not depending Du, for any small positive constant  $\epsilon$ , the following estimates hold,

$$(-u)^{1+\epsilon}\Delta u \le C.$$

Here, constant C depends on the domain  $\Omega$ , k, the function f, and  $\sup_{\Omega} |\nabla u|$ . We concentrate on the interior  $C^2$  estimates for the following Dirichlet problem for k-Hessian equations,

$$\begin{cases} \sigma_k[D^2 u] &= f(x, u, Du), \\ u|_{\partial\Omega} &= \phi. \end{cases}$$
(2)

Here,  $\Omega \subset \mathbb{R}^n$  is a bounded domain, u is a smooth function, Du and  $D^2u$  are its gradient and Hessian respectively. The k-Hessian equation:  $\sigma_k\{D^2u\} = f$  in  $\Omega$ , where  $1 \leq k \leq n$ ,

$$\sigma_k\{D^2u\} = \sigma_k\{\lambda\}$$

 $\lambda = (\lambda_1, \cdots, \lambda_n)$  are the eigenvalues of the Hessian matrix  $(D^2 u)$ , and

$$\sigma_k\{\lambda\} = \sum_{i_1 < i_2 < \dots < i_k} \lambda_{i_1} \cdots \lambda_{i_k}$$

is the k-th elementary symmetric polynomial. The k-Hessian equation includes the Poisson equation  $-\Delta u = f, (k = 1)$  and the Monge-Ampére equation  $\det(D^2 u) = f, (k = n)$  as special examples. Firstly, I will talk about k = 2, i.e. for 2-Hessian equations, there is some constant  $\beta > 0$ , such that

$$(-u)^{\beta} \Delta u \le C.$$

Here positive constants  $\beta$  and C depend on the domain  $\Omega$ , the function f,  $\sup_{\Omega} |u|$  and  $\sup_{\Omega} |\nabla u|$ . Then, for the general k, k-Hessian equations, if the solutions are k + 1 convex, namely, function u in k+1 convex cone, we have,

$$(-u)\Delta u \leq C.$$

Here, positive constant C depends on the domain  $\Omega$ , the function f,  $\sup_{\Omega} |u|$  and  $\sup_{\Omega} |\nabla u|$ . At last, as an application of interior estimates may to prove rigidity theorem for k-Hessian equations: the entire solutions in k+1 convex cone of the equations defined in  $\mathbb{R}^n$  with quadratic growth are quadratic polynomials, where k+1 convex cone is  $\Gamma_{k+1} = \{u \in C^{\infty}(\Omega) | \sigma_i > 0, 1 \leq i \leq k+1\}$ 

#### Yasuhiro Ishituka (Kyoto University)

Some geometric aspects of 2-descent of hyperelliptic Jacobians

#### Keywords: 2-descent, hyperelliptic curve, Jacobian variety

Abstract: Let us consider an abelian variety A over  $\mathbb{Q}$ , e.g. an elliptic curve over  $\mathbb{Q}$ , or the Jacobian variety of a smooth hyperelliptic curve over  $\mathbb{Q}$ . The rational points of A gives a finitely generated abelian group, called the Mordell-Weil group of A. This group has been important and mysterious objects in arithmetic geometry. We concentrate on the following question: how can we compute the rank of Mordell-Weil group explicitly? A method called descent method gives a partial solution to this question. In this talk, we firstly describe the 2-descent method for the Jacobian variety  $J_C$  of a smooth hyperelliptic curve C over  $\mathbb{Q}$ . In the process, we will obtain varieties possessing some arithmetic information of  $J_C$ . We discuss the property of the varieties, or their variants.

# 16:40-17:10

#### Chong Tian (Fudan University)

#### Unstability of pseudoharmonic maps between pseudo-Hermitian manifolds

#### Keywords: Pseudo-Hermitian manifold, Weingarten map, unstable pseudoharmonic map

Abstract: As known to all, a harmonic map is a critical point of the energy integral. A harmonic map is called stable if it has nonnegative second variation, that is, the index of the map is 0. The stability problem is an important problem in the theory of harmonic maps. R.T. Smith estimated the index of the identity map of a Riemannian manifold, in particular, he showed that the identity map on  $S^m$  is m + 1. Y.L. Xin proved that for  $m \geq 3$ , any nonconstant harmonic map  $f: S^m \to N^n$  is unstable. A result of Leung states that any nonconstant map from a compact Riemannian manifold to the sphere is unstable too. R. Howard and S. W. Wei extended the Leung's result to the case that the target manifold is a compact immersed submanifold of Euclidean space.

In recent yeas, some pseudoharmonic maps were introduced in the field of pseudo-Hermitian geometry. Petit introduced a new horizontal energy functional. He derived the first variation formula and called a critical point of the energy a pseudoharmonic map. Note that there is an extra condition on the pull-back of the torsion on the target manifold. Dong modified Petit's variational problem slightly by restricting the variational vector field to be horizontal. The critical point of the restricted variational problem about is referred to as a pseudoharmonic too. Among other results, Dong derived the second variation formula of pseudoharmonic maps into Sasakian manifold and proved that any nonconstant horizontal pseudoharmonic map from a closed pseudo-Hermitian manifold into the odd dimensional sphere is unstable.

In today's talk, I want to introduce some work with my advisor Professor Dong and Y. B. Ren. We extend the above results to the case that the target manifold is an isometric embedded CR manifold or a pseudo-Hermitian immersed submanifold of Heisenberg group and give a low bound of the index of identity map  $I: S^{2n+1} \to S^{2n+1}$  with  $n \ge 1$ . Firstly, we derive the second variation formula of pseudoharmonic maps into any pseudo-Hermitian manifolds. Then we give a condition on Weingarten map which implies that there is no nonconstant horizontal pseudoharmonic map from a closed pseudo-Hermitian manifold into an isometrically embedded CR manifold. Next we consider the identity map  $I: S^{2n+1} \to S^{2n+1}$ . From the above result we known that it is unstable. Following the result of R.T.Smith we discuss the degree of the unstability and derive that  $\operatorname{Index}(I) \ge 2n+2$ . In the end, we give a condition on CR Weingarten map which also implies there is no nonconstant pseudoharmonic map from a closed pseudo-Hermitian manifold into a pseudo-Hermitian derive that  $\operatorname{Index}(I) \ge 2n+2$ . In the end, we give a condition on CR Weingarten map which also implies there is no nonconstant pseudoharmonic map from a closed pseudo-Hermitian manifold into a pseudo-Hermitian immersed submanifold of Heisenberg group.

#### Kazuki Sato (Tohoku University)

The solubility of diagonal cubic equations

Keywords: Rational point, cubic surface, Selmer group

**Abstract**: Let V be a smooth cubic surface  $a_1X_1^3 + a_2X_2^3 + a_3X_3^3 + a_4X_4^3 = 0$  over  $\mathbb{Q}$ , where the  $a_i$  are nonzero rational integers. Assume that V is everywhere locally soluble, i.e. V has a  $\mathbb{Q}_p$ -rational point for all prime numbers p.

The Hasse principle does not hold for cubic surfaces in general, so we are concerned with the solubility over  $\mathbb{Q}$  of the surface V. Conjecturally, the existence of rational points is controlled by the Brauer group (some geometric object) of V. Subject to the assumption that the Tate-Shafarevich group of every elliptic curve is finite, Swinnerton-Dyer showed that under a certain local condition on the coefficients  $a_i$ , the surface V has a point over  $\mathbb{Q}$ .

In this talk, we give another condition on the coefficients for the solubility of V, assuming the finiteness of the Tate-Shafarevich group. In order to find a rational point, first of all we reduce V to two cubic curves. And then, we calculate the relevant Selmer groups of the Jacobians of two curves.

# 17:20-17:50

# Jungchan Lee (Sungkyunkwan University)

Some variational problem on almost Hermitian structures (Joint work with JeongHyeong Park (Sungkyunkwan University) and Kouei Sekigawa (Niigata University))

Keywords: Critical almost Hermitian structure, Einstein-Hilbert functional, first Chern number

Abstract: Let M be an even dimensional compact smooth manifold admitting an almost complex structure. Let  $(\lambda, \mu) \in \mathbb{R}^2 \setminus (0, 0)$ . We discuss the critical points of the functional  $\mathcal{F}_{\lambda,\mu}(J,g) = \int_M (\lambda \tau + \mu \tau^*) dv_g$  on the space of all almost Hermitian structures  $\mathcal{AH}(M)$  on M and its subspace  $\mathcal{AH}_c(M)$  with a certain positive constant c, where  $\tau$  and  $\tau^*$  are the scalar curvature and the \*-scalar curvature of (J,g), respectively. We shall give several characterizations of Kähler structure for some special classes of almost Hermitian manifolds, in terms of the critical points of the functionals  $\mathcal{F}_{\lambda,\mu}(J,g)$  on  $\mathcal{AH}(M)$ . Further, we provide the almost Hermitian analogy of the Hilbert's result on  $\mathcal{AH}_c(M)$ . We establish an integral formula for the first Chern number of a compact almost Hermitian surface. As applications of above variational problem, we derive curvature identities from the integral formula based on the fundamental fact that the first Chern number is a topological invariant.

#### Chiu-Ju Lin (National Tsing Hua University)

Competition of phytoplankton species for light with wavelength

Keywords: Competition for light, light spectrum, competitive exclusion, coexistence

**Abstract**: We study the competition of phytoplankton species for light with wavelength in a well mixed water column. Stomp et al. 2007 presented a reasonable model about phytoplankton species competition for light and each species prefers different interval of light spectrum, hence the specific absorption spectrum of each species is different. Their experimental results show that colorful phytoplankton species coexist.

We first consider the case that all species have the same specific absorption spectrum and different growth function and death rate. In this case, we conclude that the superior species competitively excludes others. Secondly, we consider two identical species competition model with different specific absorption spectrum. For simplicity, we assume that the growth function is linear. The conclusion is that either one species competitively excludes the other, or two species coexist. Bistability of two species is impossible.

# 18:00-18:30

# Chan Yong Kim (Sungkyunkwan University)

Bertrand curves in  $\mathbb{R}^3$  and  $S^3(1)$ 

Keywords: Spherical curve, Bertrand curve, spherical Bertrand curve

**Abstract**: A Frenet curve C is called a Bertrand curve if there exists another Frenet curve  $\overline{C}$ , distinct from C, and a bijection f between C and  $\overline{C}$  such that the same principal normal lines of C and  $\overline{C}$  at corresponding points coincide. Here,  $\overline{C}$  is called a Bertrand mate of C.

It is well-known that a Frenet curve C in  $\mathbb{R}^3$  is a Bertrand curve if and only if there exists a linear relation  $a\kappa + b\tau = 1$ , where  $\kappa$  is a curvature function of C and  $\tau$  is a torsion function of C when a and b are non-zero constant real numbers.

In this talk, We show many examples of curves on the unit 2-sphere  $S^2(1)$  in  $\mathbb{R}^3$  and the unit 3-sphere  $S^3(1)$  in  $\mathbb{R}^4$ . We study whether its curves are Bertrand curves or spherical Bertrand curves and provide some examples illustrating the resultant curves.

#### Liping Li (Fudan University)

Regular subspaces of Dirichlet forms

Keywords: Markov processes, regular Dirichlet form, subspaces, independent coupling

**Abstract**: Let *E* be a locally compact separable Hausdorff space, *m* be a  $\sigma$ -finite Radon measure with supp m = E on *E*. Then  $L^2(E, m)$  is a Hilbert space. A non-negative definite symmetric bilinear form  $\mathcal{E}$  densely defined on  $L^2(E, m)$  is called a Dirichlet form if it is closed and Markovian,  $\mathcal{F}$  is the domain of  $\mathcal{E}$ . We always signed  $(\mathcal{F}, \mathcal{E})$  for a Dirichlet form, resp.  $(T_t)_{t>0}, (G_\alpha)_{\alpha>0}$  for its semigroup and resolvent.  $\mathcal{E}_1(u, v) \triangleq \mathcal{E}(u, v) + (u, v)_m, \forall u, v \in \mathcal{E}_1(u, v) \in \mathcal{E}_1(u, v)$ 

 $\mathcal{F}$ . We then denote C(E) the space of all real continuous functions on E and its subspace  $C_c(E)$  (resp.  $C_b(E), C_c^1(E)$ ) with compact support (resp. bounded continuous functions, one order continuous differentiable functions). A Dirichlet form  $(\mathcal{F}, \mathcal{E})$  is called regular if  $\mathcal{F} \cap C_c(E)$  is dense in  $\mathcal{F}$  with  $\mathcal{E}_1$ -norm and dense in  $C_c(E)$  with uniform norm. The regular subspace  $(\mathcal{E}', \mathcal{F}')$  of a Dirichlet form  $(\mathcal{F}, \mathcal{F})$  is the regular Dirichlet forms that inherit the original form but possess smaller function spaces, i.e.  $\mathcal{F}' \subset \mathcal{F}$  and  $\mathcal{E}'(u, v) = \mathcal{E}(u, v)$  for any  $u, v \in \mathcal{F}'$ . The two problems we are concerned are: (1) the existence of regular subspaces of some given regular Dirichlet form; (2) the characterization of the regular subspaces of the given Dirichlet form if exists.

In this talk, one of our main results is that regular subspaces must inherit the jumping and killing measures of the original one. As it is well known that every regular Dirichlet form has a Beurling-Deny type decomposition which is composed by a strongly local part  $\mathcal{E}^{(c)}$ , the non-local part  $\frac{1}{2}\int (u(x)-u(y))^2 J(dxdy)$  and the killing part  $\int u(x)^2 k(dx)$  where J and k are called the jumping and killing measures of the Dirichlet form. We will show that if  $\mathcal{F}'$  is a regular subspace of Dirichlet form  $(\mathcal{E}, \mathcal{F})$ , then their jumping and killing measures in Beurling-Deny decomposition must be the same.

We also proved that an arbitrary finite dimensional Lévy type Dirichlet form with present strong local part always have proper regular subspaces. This is an extended result of one dimensional Brownian motion or diffusions by Fang, Fukushima and Ying in 2005. In particular, the regular subspaces of multidimensional Brownian motion can be generated by the coupling of one-dimensional case. In use of the killing, time change, and spatial transformations, we can also extend similar results to planar Brownian motions on any domains. We also proved that the Dirichlet forms of arbitrary symmetric finite-dimensional uniform ellipticity diffusion always possess proper regular subspaces.

# Thursday, 23 January

# 9:00-9:30

# Yong Hu (Fudan University)

Inequality of Noether type for smooth minimal 3-folds of general type

#### Keywords: Noether inequality, 3-folds

Abstract: In algebraic geometry, it is very interesting to find the relationships between the birational invariants of algebraic varieties. Given a nonsingular projective variety X, denote by  $K_X$  the canonical divisor. Let C be a smooth projective curve of genus g, then we have the equality  $\deg(K_C) = 2(g-1)$ . Let S be a smooth minimal projective surface of general type, then we have the classical Noether inequality  $K_S^2 \ge 2\chi(O_S) - 6$ . Since Noether inequality plays a very important role in the surface theory, especially in studying the geography of algebraic surfaces, we want to find the inequality of Noether type in high dimension. Let X be a smooth minimal projective 3-fold of general type. We give a sharp inequality of Noether type between the canonical volume  $K_X^3$  and  $\chi(\omega_X)$ :

$$K_X^3 \ge \frac{4}{3}\chi(\omega_X) - 2.$$

#### Kota Uriya (Tohoku University)

Asymptotic behavior of a solution to a system of quadratic nonlinear Schrödinger equations in two dimensions

Keywords: Nonlinear Schrödinger equation, Scattering theory

**Abstract**: We are concerned with the asymptotic behavior in time of a solution to a system of quadratic nonlinear Schrödinger equations in two dimensions. We say that the solution of nonlinear Schrödinger equation is asymptotically free when the solution behaves a solution of the free Schrödinger equation as time tends to infinity. In general, quadratic nonlinearities are critical in two dimensions, that is, it is not clear whether there exists an asymptotically free solution or not. It is known that the parameters which stand for the mass of the particles influence to the behavior of the solutions. Under the special relation for that parameter, we show the existence of the solution to the system which is neither asymptotically free nor modified free solution.

#### 9:40-10:10

#### Jian Xiao (Fudan University)

Weak transcendental holomorphic Morse inequalities on compact Kähler manifolds

#### Keywords: Holomorphic Morse inequalities, Kähler current, big cohomology class

Abstract: Let X be an n-dimensional compact complex manifold and let  $\alpha, \beta$  be two cohomology classes in the nef cone of X. For n-dimensional projective varieties, a k-cycle is called nef if its intersection number with any effective (n-k)-cycle is non-negative, and it is called big if it lies in the interior of cone generated by effective k-cycles. We also have similar nefness or bigness defined by metric over general compact complex manifolds.

If X is a smooth complex algebraic variety and  $\alpha, \beta$  are Chern classes of line bundles, a basic theorem of Siu tells us if  $\alpha^n - n\alpha^{n-1}\beta > 0$  then  $\alpha - \beta$  is big. Similar to Siu's theorem, X.Y.Yuan has also proved the same big criterion for arithmetic varieties.

In my talk, I will introduce Demailly's remarkable holomorphic Morse inequalities. We shall see Siu's result can be derived from holomorphic Morse inequalities. But rationality is important in the previous results. For general k, I will give a big criterion for the class  $\alpha^k - \beta^k$  on compact Kähler manifolds without projective or rational conditions. Our results partially improve the recent results of Boucksom-Demailly-Paun-Peternell.

# Xu Qing (Fudan University)

# Backward Stochastic Schrödinger Equations and related topics

Keywords: Backward stochastic differential equation, schrödinger equation

**Abstract**: In this speech, a class of backward stochastic differential equations of schrödinger type is studied. First, we will introduce the field of Backward Stochastic Differential Equations (BSDE, for short) and give the definition of the adapted solution of the Backward Stochastic Schrödinger Equations. In the linear case, both of the additive and multiplicative noises are considered. We derive the global existence and uniqueness of the adapted solution via the Galerkin method. We also consider some nonlinear cases. In these cases, the local existence and uniqueness of the solution is derived via the Strichartz estimate of the schrödinger operator. We will also present some other results, e.g., how the solution behaves when the time approaches the terminal.

#### 10:20-10:50

#### Yen-Wen Fan (National Taiwan University)

## An Optimal Gap Theorem in a Complete Strictly Pseudoconvex CR (2n + 1)-Manifold

#### Keywords: Gap Theorem, Linear Trace Harnack, CR manifold

Abstract: In the Kaehler geometry, it is conjectured that a complete noncompact Kaehler manifold M of positive holomorphic bisectional curvature of complex dimension m is biholomorphic to  $\mathbb{C}^m$ . The first result concerning this conjecture was obtained by Mok-Siu-Yau. They proved that M is isometrically biholomorphic to  $\mathbb{C}^m$  with the standard flat metric under assumptions of maximum volume growth condition  $V(r) \geq \delta r^m$  and the scalar curvature R decays as  $R = o(r^{-2-\epsilon})$ . We call this theorem as a gap theorem. (The "gap" indicates "how big the curvature can be" between flat and not flat manifold and try to find an constraint for curvature so that the manifold is flat.) For a long time, it has been conjectured the maximum volume growth condition was not necessary. In 2012, L. Ni obtained an optimal gap theorem on M with nonnegative bisectional curvature without the maximum volume growth condition, provided the average of scalar curvature decay as  $o(r^{-2})$ . The same question can be asked in the CR manifold category. Now let M be a (2n + 1)-manifold with a contact structure and a complex structure J on the contact plane. One can view it as a boundary of a convex domain in  $\mathbb{C}^m$ . Under the same curvature assumption, we are able to generalize the optimal gap theorem to the CR manifold when torsion is vanishing. The classification of CR geometry is rare and most result is compact. This result is the first result about the complete manifold with CR structure. In this talk I will give a review of CR geometry and history. And then I will sketch the idea of the proof. This is an application of linear trace Li-Yau-Hamilton inequality of Lichnerowicz-Laplacian heat equation.

#### Makoto Fujiwara (Tohoku University)

#### Uniform and constructive provability in reverse mathematics

Keywords: Reverse mathematics, Uniformity of proofs, Constructive mathematics, Metatheorem

Abstract: Reverse mathematics is a research program in foundation of mathematics, which was initiated by H. Friedman in the 1970's and extensively developed by S. Simpson and others. In reverse mathematics, we seek the necessary set existence axiom for proving each theorem in ordinary mathematics. In this way, most of ordinary theorems are classified into three kinds. However, it is known that the classification will slightly change if we stand on the position that a proof of theorem "For any X satisfying some conditions, there exists Y satisfying some conditions" is required to give the uniform construction of Y from X. We say that a proof is uniform if such a construction is given.

Recently, some interesting metatheorems, which are useful to show the constructive unprovability of theorems by using the uniform consideration in Friedman-Simpson reverse mathematics, have been established. This kind of metatheorems can be a bridge between the research of reverse mathematics and that of constructive mathematics. In this talk, I will present an overview of such metatheorems and their application to actual mathematical theorems in some examples.

#### 11:00-11:30

# Masatoshi Kitagawa (The University of Tokyo) Stable branching laws for spherical varieties

Keywords: Lie group, spherical variety, multiplicity-free representation

Abstract: Let G be a connected reductive algebraic group over  $\mathbb{C}$  (e.g.  $\operatorname{GL}(n,\mathbb{C}), \operatorname{Sp}(n,\mathbb{C}),\ldots$ ), and X be a quasi-affine G-variety over  $\mathbb{C}$ . We consider a  $(\mathbb{C}[X], G)$ -module V, and decompose V into the direct sum of irreducible representations of G as  $V = \bigoplus_{\lambda} m(\lambda)\pi_{\lambda}$ . Here,  $\mathbb{C}[X]$  is the ring of regular functions on X. Our main concern is to compute the multiplicities  $m(\lambda)$ . X is said to be spherical if  $\mathbb{C}[X]$  is multiplicity-free Gmodule (i.e.  $m(\lambda) \leq 1$  for  $V = \mathbb{C}[X]$ ). F. Sato gave a method to describe  $m(\lambda)$  for 'sufficiently large'  $\lambda$ , when X is a affine spherical homogeneous space and V is the space of global sections of a G-equivariant vector bundle on X.

In this talk, we generalize Sato's theorem for any quasi-affine spherical variety X and  $(\mathbb{C}[X], G)$ -module V. As an application, we will treat branching laws of infinite dimensional unitary representations of Lie groups, called holomorphic discrete series representations.

#### Jinyeong Park (Seoul National University)

Practical synchronization of Kuramoto system with an intrinsic dynamics

**Keywords**: Kuramoto model, intrinsic dynamics, external force, practical synchronization

**Abstract**: We study the practical synchronization of the Kuramoto dynamics of processors distributed over networks. The processor dynamics on the nodes of the network are governed by the interplay between their own intrinsic dynamics and Kuramoto coupling dynamics. We present two sufficient conditions for practical synchronization under homogeneous and heterogeneous forcing. For practical synchronization estimates, we employ the configuration diameter as a Lyapunov functional, and derive a Gronwall-type differential inequality for this value.

# 11:40-12:10

#### Yuichiro Tanaka (The University of Tokyo)

Visible actions on generalized flag varieties and a generalization of the Cartan decomposition

**Keywords**: multiplicity-free representation; compact Lie group; flag variety; visible action; Cartan decomposition

**Abstract**: I would like to talk about normalization of matrices motivated by the theory of visible actions on complex manifolds, which was introduce by T. Kobayashi.

Let H be a Lie group and X a complex manifold with a holomorphic H-action. We say the action  $H \curvearrowright X$  is strongly visible if

- there is a real submanifold S of X such that  $X' := H \cdot S$  is an open subset of X, and
- there is an anti holomorphic diffeomorphism  $\sigma$  of X' such that  $\sigma(H \cdot x) \subset H \cdot x$  for  $x \in X'$  and  $\sigma|_S = \mathrm{id}_S$ .

If X is a homogeneous space G/L of a matrix group G, the visibility of the H-action on G/L implies that any element of G can be normalized to certain form corresponding to the totally real submanifold S by using the right L-action and the left H-action on G.

In this talk, we consider normalization of elements of compact Lie groups (the unitary group, the orthogonal group, the symplectic group, etc) under the left and right actions of Levi subgroups (block diagonal matrix subgroups).

### Eun-Kyung Kim (Ewha Woman's University)

Relations between Multilinear Maps and Fully Homomorphic Encryption Scheme

Keywords: Ideal lattice, Multilinear map, Fully homomorphic encryption

Abstract: Bilinear maps are one of the most important and useful tools in cryptography including one-round 3-way secret key exchange protocol which was introduced by Joux in 2000. Multipartite key exchange protocol is one of the main interest of many researchers, so from the tripartite key exchange protocol construction of Joux, they expect that  $\kappa$ -multilinear maps may allow to have one-round ( $\kappa + 1$ )-way secret key exchange protocol. However, extending bilinear maps to multilinear had been an important open problem.

Another important and useful tools in cryptography is a fully homomorphic encryption. Like multilinear maps, it also has many applications. The first fully homomorphic encryption scheme was introduced by Gentry in 2009, and it also used ideal lattice. After that, in 2010 Dijk et. al constructed simpler fully homomorphic encryption scheme over integers. The first plausible candidate of multilinear maps was constructed by Garg et. al in 2013 and it is from ideal lattice and then Coron et. al presented a different construction that works over the integers in 2013.

In this talk, we review the multilinear map and fully homomorphic encryption scheme over integers briefly and present some relations between these schemes.

# Friday, 24 January

# 9:30-10:30

# Shanjian Tang (Fudan University)

Linear-Quadratic Optimal Control: from deterministic to stochastic

**Keywords**: linear-quadratic regulator, Kalman filter, Riccati equation, Hamilton system, explicit solution, backward stochastic Riccati equation

**Abstract**: In this talk, I would begin with the historical contribution of R. E. Kalman on linear quadratic regulator for a deterministic ordinary differential system, where in particular the solution of Riccati equation is explicitly represented via the transition matrix of the related deterministic Hamilton system. Then, we consider the stochastic differential system, recall Kalman filter, and review the related works by W. M. Wonham, J. M. Bismut, and others on the stochastic linear quadratic (SLQ) control. We shall show that how the solution of the Riccati equation should satisfy a system of matrix-valued NONLINEAR ODEs when the coefficients of the stochastic linear quadratic control problem are all deterministic.

Finally, we consider a robust SLQ control problem and expose the difficult features of the associated backward stochastic Riccati equation.

# 10:40-11:40

#### Seok-jin Kang (Seoul National University)

#### Cyclotomic categorification theorem and 2-representation theory

Keywords: categorification, Khovanov-Lauda-Rouquier algebra, 2-representation theory

**Abstract**: In this talk, we will first explain the main idea of categorical representation theory. One of the most prominent applications is LLT-Ariki theory where affine Hecke algebras and their cyclotomic quotient categorify quantum affine algebras of type A and their highest weight modules.

In 2008, Khovanov-Lauda and Rouquier independently introduced a family of graded algebras which are now called the Khovanov-Lauda-Rouquier algebras or quiver Hecke algebras. The KLR algebras can be regarded as a vast generalization of affine Hecke algebras. It was shown by Khovanov-Lauda and Rouquier that they give a categorification of quantum Kac-Moody algebras. Recently, Kang and Kashiwara showed that the cyclotomic quotients of KLR algebras provide a categorification of integrable highest weight modules over quantum Kac-Moody algebras.

Finally, we will discuss possible applications of these categorification theorems and future developments in this area.

# 13:40-14:10

#### Yuuya Takayama (Research Institute for Mathematical Sciences)

Introduction to bow varieties

Keywords: hyper-Kähler manifold, bow variety, quiver variety

Abstract: (M, g, I, J, K) is called a hyper-Kähler manifold, if M is a 4n-dimensional manifold, I, J, K (= IJ) are complex structures and g is a Kähler metric for I, J, K. Since this definition is strict, so few explicit examples are well-known. On the other hand, we can construct some other hyper-Kähler manifolds from explicit examples by hyper-Kähler quotients. And quiver varieties and bow varieties, appearing in Keywords, are classes of hyper-Kähler quotients. Then there exists a question what manifolds are constructed by hyper-Kähler quotients. The answer is well-known for quiver varieties, but it was not known for bow varieties. In this talk, I will explain the way to construct bow varieties, the reason to introduce them, and a partial answer to the above question for them.

# Ye Li (Tsinghua University)

A class of nonconforming quadrilateral finite elements for incompressible flow

**Keywords**: Incompressible flow, finite element method, nonconforming quadrilateral elements, optimal error estimates

**Abstract**: I have been studying the numerical methods for PDEs. The finite element method is a class of numerical methods for solving PDEs. It is a combination of variational methods and subdivision interpolation technique and it is widely used in engineering. We say an element is nonconforming if its finite element space does not belong to the original space for the continuous variational problem. The Navier-Stokes equations are used to describe incompressible flow. In this talk I will focus on the low-order nonconforming rectangular and quadrilateral finite elements approximation of incompressible flow. Especially I consider the problem: which kinds of basis functions are to be chosen in order to have an optimal low-order error estimate on quadrilateral meshes?

Beyond the previous research works, we propose a general strategy to construct the basis functions. Under several specific constraints, the optimal error estimates are obtained, i.e., the first order accuracy of the velocities in  $H_1$ -norm and the pressure in  $L_2$ -norm, as well as the second order accuracy of the velocities in  $L_2$ -norm. Besides, we clarify the differences between rectangular and quadrilateral finite element approximation. In addition, we give several examples to verify the validity of our error estimates.

# 14:20-14:50

# Yusuke Nakamura (The University of Tokyo)

Minimal model program and singularity theory

Keywords: Minimal model program, termination of flips, singularity theory

**Abstract**: One of the most important problem in algebraic geometry is the birational classification of algebraic varieties. The minimal model program is a "program" whose goal is to find a variety which is as simple as possible in a birational equivalent class. In this area, the conjecture of terminations of flips is one of the most important conjecture, which certifies that the program really ends in the finite steps.

The conjecture of terminations of flips is a global geometrical problem in essentials. The minimal log discrepancy (mld for short) was introduced by Shokurov, in order to reduce the conjecture of terminations of flips to a local problem about singularities. Recently, this has been a fundamental invariant in the minimal model program. There are two related conjectures about mld's, the ACC (ascending chain condition) conjecture and the LSC (lower semi-continuity) conjecture. Shokurov showed that these two conjectures imply the conjecture of terminations of flips.

In this talk, we will explain the above conjectures and the relation to the termination of flips. After that, we will explain the known results about these conjectures.

## Jihoon Ok (Seoul National University)

 $L^{p(\cdot)}$ -regularity theory for the gradient of weak solutions for elliptic and parabolic equations in divergence form

**Keywords**:  $L^{p(\cdot)}$ -estimate, elliptic equation, parabolic equation

Abstract: Recently there have been systematic and extensive research activities on generalized Lebesgue and Sobolev spaces with variable exponents,  $L^{p(\cdot)}$  and  $W^{1,p(\cdot)}$ . These spaces have been developed from the classic Lebesgue and Sobolev spaces. They appear in the literature dealing with physical phenomena where the energies have the nonstandard growths in the area of various applications, for examples, the eletrorheological fluid, the thermistor problem, image processing models and so on. In this talk, I will show an optimal  $L^{p(\cdot)}$ -regularity theory for the gradient of weak solutions for elliptic and parabolic equations in divergence form with measurable coefficients in a nonsmooth domains. With a variable function  $p(\cdot)$  satisfying log-Hölder continuity, we prove that the gradient of weak solution is as integrable as the nonhomogeneous term in  $L^{p(\cdot)}$  spaces under the assumptions that the coefficients are merely measurable in one variable while have a small bounded mean oscillation(BMO) in the other variables, and that the domain is assumed to be  $\delta$ -Reifenberg flat.

#### 15:00-15:30

## Yuhei Suzuki (The University of Tokyo)

# Amenable minimal Cantor systems of free groups arising from diagonal actions

Keywords: C\*-algebras, amenable actions, free groups, Cantor systems

Abstract: The notion of the amenability for topological dynamical systems is a natural generalization of the one for discrete groups. Amenability of dynamical system is characterized by the nuclearity (a notion of the amenability in  $C^*$ -algebra theory) of an associated  $C^*$ -algebra, called the reduced crossed product. Amenability

also provides other nice properties for the reduced crossed product. From this, we are interested in amenable dynamical systems in particular. In this talk, we consider amenable minimal Cantor systems of free groups. The motivation comes from the following two natural asks. The first one is how well the crossed products remember the original dynamical systems. The second one is giving new (tractable and useful) presentations for Kirchberg algebras. Here a Kirchberg algebra is a C\*-algebra satisfying certain nice properties. (More precisely, a C<sup>\*</sup>-algebra A is said to be a Kirchberg algebra if it is simple, separable, nuclear, purely infinite, and satisfying the UCT.) It is known that Kirchberg algebras are completely classified by K-theoretic invariants. (The classification theorem of Kirchberg and Phillips.) Hence they are very important and interesting. To find the answers of both questions, it is important to give many concrete examples whose crossed products are completely determinable. However, until now, only a few examples were known. (E.g., the boundary action, the dynamical system constructed by Elliott-Sierakowski.) In my recent work, I construct continuum many examples of amenable minimal Cantor systems of free groups whose crossed products are Kirchberg algebras and their K-groups are completely determined (hence their isomorphism classes themselves are also completely determined thanks to the classification theorem of Kirchberg and Phillips). Moreover, with a little effort, we also construct such systems for virtually free groups. Then, as a consequence, we obtain certain (continuum many) Kirchberg algebras are decomposed as a crossed product of an amenable minimal (topologically free) Cantor system of arbitrary virtually free groups. Furthermore, in this computation, the technique of computations for K-groups for certain amenable minimal Cantor systems are also established. I also want to talk about an application to the classification for certain amenable minimal Cantor systems of free groups.

#### Jinsu Kim (Seoul National University)

#### Efficient Fully Homomorphic Encryption

**Keywords**: ElGamal, Goldwasser-Micali, Naccache-Stern, Hybrid Scheme, Multiplicative Homomorphic Encryption, Additive Homomorphic Encryption, Fully Homomorphic Encryption, Decryption Circuit, Exponentiation, Bootstrapping

**Abstract**: The concept of computation on encrypted data without decryption was firstly introduced by Rivest, Adleman and Detourzos in 1978. After thirty years, Gentry proposed a fully homomorphic encryption (FHE) based on ideal lattices. This scheme is far from being practical due to its large computation costs and large ciphertexts. Since then, lots of efforts has been done to devise more efficient schemes and their successors become much more efficient. However, most FHE schemes still have huge ciphertext size, at least millions of bits for a single ciphertext. This is a big bottleneck when it is deployed in practice.

In this talk, we explore how to obtain efficient hybrid homomorphic encryption schemes by combining a public key encryption with small ciphertext size and a somewhat homomorphic encryption (SHE) that could evaluate the decryption circuit of the PKE. For efficient construction, we consider SHE for hybrid scheme rather than FHE.

#### 16:00-16:30

#### Bo Li (Tsinghua University)

Infinitely many solutions for the prescribed curvature problem of polyharmonic operator

Keywords: Polyharmonic operator, critical exponents, infinitely many solutions

Abstract: We study the existence of infinitely many solutions for the prescribed curvature problem  $D_m u = K|u|^{m^*-2}u$  in  $\mathbb{S}^N$ . The number  $m^* = \frac{2N}{N-2m}$  is called the critical exponent, where  $N \ge 2m+1$ ,  $m \ge 1$ .  $D_m$  is the polyharmonic operator of 2m order given by  $D_m = \prod_{k=1}^m (-\Delta_g + \frac{1}{4}(N-2k)(N+2k-2))$ . Given a compact Riemannian manifold  $(\mathbb{S}^N, g)$  and a smooth function K defined on  $\mathbb{S}^N$ , the prescribed

Given a compact Riemannian manifold  $(\mathbb{S}^N, g)$  and a smooth function K defined on  $\mathbb{S}^N$ , the prescribed curvature problem of polyharmonic operator is to find a conformally invariant metric  $g_u = u^{\frac{4}{N-2m}}g$  such that the scalar curvature is just K under this new metric  $g_u$ .

Under what condition of K shall we obtain infinitely many solutions to the prescribed curvature problem of polyharmonic operator? In this talk, we will give the positive answer to this question. First, we assume K has a positive maximum between the poles, and show the existence of infinitely many non-radial positive solutions by energy expansion and min-max methods. Then, we assume K is a positive constant instead, the problem allows infinitely many non-radial sign-changing solutions by glueing large amounts of bubble solutions.

### Tse-Chung Yang (National Taiwan University)

Monomial, Gorenstein, and Bass orders

Keywords: Maximal orders, monomial orders, Gorenstein orders, Bass orders

**Abstract**: In the integral theory for central simple algebras over non-Archimedean local fields, we have the following important classes of orders: maximal orders, hereditary orders, Bass orders and Gorenstein orders. Many theories and relations are investigated by many authors for understanding these classes of orders, as well as their module structures. It is well-known that they form the following proper inclusions:

 $(maximal orders) \subset (hereditary orders) \subset (Bass orders) \subset (Gorenstein orders)$ 

In this talk, we study a class of orders called monomial orders in a central simple algebra over a non-Archimedean local field. Monomial orders are easily represented and they may be also viewed as a direct generalization of Eichler orders in quaternion algebras. A criterion for monomial orders to be Gorenstein or to be Bass is given. It is shown that a monomial order is Bass if and only if it is either a hereditary or an Eichler order of period two.

# 16:40-17:10

# Sz-Sheng Wang (National Taiwan University)

Calabi-Yau threefolds with small contractions

Keywords: Calabi-Yau threefold, primitive contraction

Abstract: Let X be a projective Calabi-Yau 3-fold. A primitive contraction of X is a birational contraction onto a normal projective variety which cannot be further factored into birational morphisms of normal varieties. In order to study the behaviour of the Kähler cone under deformations, P.M.H. Wilson gives a coarse classification of such contractions. A primitive contraction is called of type I if it is a small contraction, i.e. it contracts a finite number of curves to points. In this talk, we will prove that a primitive type I contraction is irreducible, i.e. every fiber is either a point or a irreducible curve, and study Calabi-Yau threefolds with small contractions. We will also discuss applications to extremal transition if time allowed.

# Nobuaki Naganuma (Tohoku University)

Asymptotic error distributions of the Crank-Nicholson scheme for SDEs driven by fractional Brownian motion

**Keywords**: Fractional Brownian motion, Stochastic differential equation, Crank-Nicholson scheme, Exact rate of convergence

**Abstract**: We investigate the error between the solution to a stochastic differential equation(SDE) driven by a fractional Brownian motion and the approximation by the Crank-Nicholson scheme associated to the equation.

In preceding results, researchers deal with numerical schemes solving SDEs, for example, the Crank-Nicholson scheme and the Euler scheme. They are interested in the convergence rates of the errors and the limit distribution, which is the limit of the errors with some weights.

In this talk, we consider the error of the Crank-Nicholson scheme as stochastic processes and determine the convergence rate and the limit distribution in the Skorohod topology. The limit distribution is expressed in terms of the solution to the equation and the Itô integral with respect to a standard Brownian motion independent of the driving process of the equation. The key ingredients in our proof are asymptotic behavior of weighted Hermite variations as stochastic processes.

#### 17:20-17:50

# Qizhi Wang (Fudan University)

Conformal Positive Mass Theorem for Asymptotically Flat Manifolds with Inner Boundary

#### Keywords: Mass, conformal, spin

**Abstract**: Inspired by Witten's insightful spinor proof of positive mass theorem in general relativity, in this talk, we will use the spinor method to derive higher dimensional type conformal positive mass theorems on asymptotically flat spin manifolds with inner boundary, which states that under a condition about the plus (minus) relation between the scalar curvatures of the original and the conformal manifold, in addition with some boundary condition, we will get the associated positivity of their ADM masses. The rigidity part of the plus part without boundary is used in the proof of black hole uniqueness theorems. These theorems are also related with quasi-local mass and the spectrum of Dirac operator. We will talk about the spinor method

first, and use it to prove the main theorem, then we will briefly talk about their relation with quasi-local mass (Brown-York mass) and Dirac spectrum in asymptotically flat manifold with inner boundary.

# Cheng-Fang Su (National Central University)

The existence of solutions of 2-dimensional incompressible Navier-Stokes equations on a moving domain in an optimal Sobolev space

Keywords: Incompressible Navier-Stokes equations, ALE formulation, moving domain

**Abstract**: We establish the existence of a solution to the Navier-Stokes equations on a moving domain with surface tension in an optimal Sobolev space for the case of two space dimension. No compatibility conditions are required to guarantee the existence of a solution.

In this talk, we will introduce the ALE formulation which can transform our moving domain into a fixed domain and simplify our problem. However, the ALE formulation could make nonlinear terms of Navier-Stokes equations stronger. So we will give an simple example to explain the difficulties of our study.