THE UNIVERSITY  OF HONG KONG

Institute of Mathematical Research
Department of Mathematics

The 2024 Information Theory Month

Venue: 210, Run Run Shaw Building, HKU

Time	Event	Speaker	Affiliation
Mini-workshop 1 August 09, 2024 (Friday) Chaired by Jun Su			
3:00 – 4:00 pm	*Isoperimetry and Concentration in Product Polish Spaces*	Lei Yu	Nankai University
4:10 – 5:10 pm	*A Semigroup Approach to Talagrand-Type Isoperimetric Inequalities*	Peijie Li	The University of Hong Kong
5:20 – 6:20 pm	*Sequential Quantum Hypothesis Testing*	Yonglong Li	Xi'an Jiaotong University
Mini-workshop 2 August 16, 2024 (Friday) Chaired by Peijie Li			
3:00 – 4:00 pm	*Simulation under Renyi Divergences*	Lei Yu	Nankai University
4:10 – 5:10 pm	*Shift of Finite Types Obtained by Forbidding One Block*	Chengyu Wu	The University of British Columbia
5:20 – 6:20 pm	*Supervised Factor Modeling for High-Dimensional Linear Time Series*	Guodong Li	The University of Hong Kong
Mini-workshop 3 August 23, 2023 (Friday) Chaired by Peijie Li			
3:00 – 4:00 pm	*Feedback Capacity of the Continuous-Time ARMA(1,1) Gaussian Channels*	Jun Su	The University of Hong Kong
4:10 – 5:10 pm	*Minimax Parameter Estimation in Restricted Parameter Space for High-Dimensional Data*	Shao-Lun Huang	Tsinghua-Berkeley Shenzhen Institute
5:20 – 6:20 pm	*Asymptotic Capacity of 1-Bit MIMO Channels: From Bayesian Statistics to Large-Scale MIMO Communications*	Sheng Yang	CentraleSupelec, Paris-Saclay University
Mini-workshop 4 August 30, 2023 (Friday) Chaired by Jun Su			
3:00 – 4:00 pm	*MacWilliams Extension Property with Respect to Weighted Poset Metric*	Yang Xu	Fudan University

4:10 – 5:10 pm	*Introduction to Zero Knowledge Proof*	Haibin Kan	Fudan University

Titles and Abstracts

August 09, 2024 (Friday)

Lei Yu Nankai University
Isoperimetry and Concentration in Product Polish Spaces

The isoperimetric problem is one of most classic problems, which is to minimize the boundary-size (i.e., perimeter) of a set when the size (i.e., volume) of the set is given. A famous result for the isoperimetric problem in the n-dimensional Euclidean space states that an n-ball has the smallest surface area per given volume. However, the isoperimetric problem in other spaces is widely open. In this talk we focus on the isoperimetric problem for product probability measures on Polish metric spaces. We illustrate how to combine information-theoretic and optimal-transport-theoretic techniques to derive exponentially sharp bounds for the isoperimetric problem

Peijie Li The University of Hong Kong
A Semigroup Approach to Talagrand-Type Isoperimetric Inequalities

Isoperimetric inequalities are essential in characterizing the high-dimensional behavior of Boolean functions. Specifically, this talk focuses on Talagrand-type isoperimetric inequalities, collectively including the Poincare inequality, the KKL inequality, and several celebrated inequalities proposed by Talagrand. Drawing inspiration from Elden and Gross's resolution of an isoperimetric inequality conjectured by Talagrand, we present a general approach for establishing Talagrand-type isoperimetric inequalities by analyzing the semigroup of noise operators on Boolean functions.

Yong Long Li Xi'an Jiaotong University
Sequential Quantum Hypothesis Testing

In this work, we consider the sequential quantum hypothesis testing problem and propose an adaptive sequential test. We then show that the proposed adaptive test is optimal in the sense of achieving the optimal error exponent. Also in this work, we show that adaptive test perform better than non-adaptive tests.

August 16, 2024 (Friday)

Lei Yu Nankai University
Simulation under Renyi Divergences

It is well known that the empirical measure of i.i.d. samples converges weakly to the law of samples as the number of samples increases. As an extension, the channel resolvability problem refers to approximating a target output distribution of a given channel when the input is chosen randomly and uniformly over a set of i.i.d. samples. Here we use the Rényi divergence to measure the level of the approximation. In this talk, we will introduce the convergence behavior of the Rényi divergence when the

number of samples increases exponentially as the dimension of the channel increases. We also connect the Rényi resolvability problem to other two simulation problems, including the common information problem (i.e., the distributed source simulation problem) and the distributed channel simulation problem.

Chengyu Wu The University of British Columbia
Shift of Finite Types Obtained by Forbidding One Block

We focus on shift of finite types (SFTs) obtained by forbidding one word from an ambient SFT. Given a word in a one-dimensional full shift, Guibas, Odlyzko and Lind showed that its auto-correlation, zeta function and entropy (of the corresponding SFT) all determine the same information. We first prove that when two words both have trivial auto-correlation, the corresponding SFTs not only have the same zeta function, but indeed are conjugate to each other, and this conjugacy is given by a chain of the so-called swap conjugacies. We extend this result to the case when the ambient SFT is the golden mean shift, with an additional assumption on the extender set of the words. Then, we introduce SFTs obtained by forbidding one finite pattern from a higher dimensional ambient SFT. We prove that, when two patterns have the same auto-correlation, then there is a bijection between the language of their corresponding SFTs. This is joint work with Nishant Chandgotia, Brian Marcus and Jacob Richey.

Guodong Li
Supervised Factor Modeling for High-Dimensional Linear Time Series

Motivated by Tucker tensor decomposition, this paper imposes low-rank structures to the column and row spaces of coefficient matrices in a multivariate infinite-order vector autoregression (VAR), which leads to a supervised factor model with two factor modelings being conducted to responses and predictors simultaneously. Interestingly, the stationarity condition implies an intrinsic weak group sparsity mechanism of infinite-order VAR, and hence a rank-constrained group Lasso estimation is considered for high-dimensional linear time series. Its non-asymptotic properties are discussed thoughtfully by balancing the estimation, approximation and truncation errors. Moreover, an alternating gradient descent algorithm with thresholding is designed to search for high-dimensional estimates, and its theoretical justifications, including statistical and convergence analysis, are also provided. Theoretical and computational properties of the proposed methodology are verified by simulation experiments, and the advantages over existing methods are demonstrated by two real examples.

August 23, 2024 (Friday)

Jun Su The University of Hong Kong
Feedback Capacity of the Continuous-Time ARMA(1,1) Gaussian Channels

We consider the continuous-time ARMA(1,1) Gaussian channel and derive its feedback capacity in closed form. More specifically, the channel is given by $y(t) = x(t) + z(t)$, where the channel input $\{x(t)\}$ satisfies average power constraint P and the noise $\{z(t)\}$ is a first-order autoregressive moving average (ARMA(1,1)) Gaussian

process satisfying $z'(t) + \kappa z(t) = (\kappa + \lambda)w(t) + w'(t)$, where $\kappa > 0$, $\lambda \in \mathrm{R}$ and $\{w(t)\}$ is a white Gaussian process with unit double-sided spectral density.

We show that the feedback capacity of this channel is equal to the unique positive root of the equation $P(x + \kappa)^2 = 2x(x + |\kappa + \lambda|)^2$ when $-2\kappa < \lambda < 0$ and is equal to $P/2$ otherwise. Among many others, this result shows that, as opposed to a discrete-time additive Gaussian channel, feedback may not increase the capacity of a continuous-time additive Gaussian channel even if the noise process is colored. The formula enables us to conduct a thorough analysis of the effect of feedback on the capacity for such a channel. We characterize when the feedback capacity equals or doubles the non-feedback capacity; moreover, we disprove continuous-time analogues of the half-bit bound and Cover's $2P$ conjecture for discrete-time additive Gaussian channels.

Shao-Lun Huang Tsinghua-Berkeley Shenzhen Institute
Minimax Parameter Estimation in Restricted Parameter Space for High-Dimensional Data

In many communication and machine learning problems, the problem of estimating system or model parameters from a large number of i.i.d. samples, such that the parameters are restricted to certain subspace of the ambient space, is often considered. In particular, we consider a minimax formulation where the goal is to search for the estimator optimizing the worst-case performance of parameter estimation subject to the given constraint. We focus on the asymptotic regime for large n, and propose a novel technique to characterize the minimax loss with respect to the optimal estimator up to the second-order term. We show that the optimal second-order convergence rate depends on the local smoothness of the Fisher information of the parametrized model and can be solved from a differential equation. Our results generalize several classical results, such as the bounded normal mean problem, and reveal the information theoretical insights in machine learning algorithm designs.

Sheng Yang Hong Kong University of Science and Technology
Asymptotic Capacity of 1-Bit MIMO Channels: From Bayesian Statistics to Large-Scale MIMO Communications

Large-scale MIMO systems utilizing low-resolution analog-to-digital converters (ADCs) have emerged as a cost-effective and energy-efficient solution for future wireless communication networks. While extended research has been conducted on signal processing and transceiver design in these systems, the fundamental Shannon capacity limit remains elusive. In this talk, we introduce a novel approach that leverages information-theoretic asymptotics from Bayesian statistics to derive the Shannon capacity of such systems. We reveal the critical role of the Fisher information and Jeffreys' prior in this characterization, and demonstrate how to apply this method to derive the asymptotic capacity of 1-bit MIMO channels in the Gaussian and the (coherent and non-coherent) fading cases.

August 30, 2024 (Friday)

Yang Xu Fudan University
MacWilliams Extension Property with Respect to Weighted Poset Metric

In 1962, MacWilliams proved that any Hamming weight preserving map between two linear codes extends to a Hamming weight isometry of the whole ambient space, which is often referred to as MacWilliams extension property (MEP) in the literature. This celebrated MacWilliams extension theorem has since been extended, generalized and discussed extensively with respect to various weights and metrics in coding theory and with respect to codes over various alphabets. Recently, there has been a growing interest in MEP concerning weights and metrics introduced by poset structures. In this talk, we consider MEP with respect to weighted poset metric, a metric first introduced by Hyun, Kim and Park in 2019 which is determined by a poset together with a weight function. Our ambient space is the Cartesian product of a finite family of left modules over a ring. We characterize the group of isometries with respect to weighted poset metric, which is used to show that MEP implies the unique decomposition property of the weighted poset. When the poset is hierarchical or the weight function is identically 1, with some weak additional assumptions, we give necessary and sufficient conditions for MEP with respect to weighted poset metric in terms of MEP with respect to Hamming metric. When the ambient space is set to be a finite dimensional vector space over a finite field, we compare MEP with various well studied coding-theoretic properties including the MacWilliams identity, reflexivity of partitions, transitivity of the group of isometries and whether the corresponding metric induces an association scheme; in particular, we show that MEP is always stronger than all the other properties. This is a joint work with Kan Haibin and Han Guangyue.

Haibin Kan Fudan University
Introduction to Zero Knowledge Proof

Zero knowledge proof is an important cryptographic tool used to prove that a statement is true without revealing any additional information. This proof system has a wide range of applications in protecting personal privacy and data security. The first part of this report introduces the basic concepts, principles, and applications of zero knowledge proofs, and discusses some classic zero knowledge proof protocols. The second part simply introduces the design of a new zero knowledge proof protocol under the flow model. At present, the memory overhead of the prover in zero knowledge proof protocols is a major bottleneck for applications. In the stream model, the prover can read in the required data as needed without having to load all the data into memory at once.