2018年

九州大学 組合せ数学セミナー

Hakata Workshop 2018; Summer Meeting[1]

下記のようにセミナーを開催しますので, ご案内申し上げます。

世話人:
溝口 佳寛（九大 IMI）
島袋 修（長崎大）
栗原大武（北九州高専）
三枝崎　剛 (琉球大)
谷口 哲至（広島工大)
田上 真（九州工大）
千葉周也 (熊本大)
Daniel GAINA(九州大)

アドバイザー： 坂内 英一

記

日時: 2018年6月16日 (土) 13:27–17:35

場所: February 23, Seminar Room P (4F) in Reference Eki Higashi Building. 1-16-14 Hakata-Eki-Higashi, Hakata-Ku, Fukuoka City, 812-0013.

プログラム

13:27–13:30 Opening （Tetsuji Taniguchi）

13:30-14:10 Yota Otachi (Kumamoto University)
Space-efficient algorithms for longest increasing subsequence

14:20-15:00 Yuta Watanabe (National Institute of Technology, Ube college)
Association schemes on the Schubert cells of a Grassmannian

15:10-15:50 Hajime Tanaka(Tohoku University)
The Terwilliger algebra with respect to an edge of a bipartite 2-homogeneous distance-regular graph

16:00-16:40 Akihiro Munemasa (Tohoku University)
A graph with smallest eigenvalue -3 related to the shorter Leech lattice

16:50-17:30 Kenichi Arai(Nagasaki University)
Computer-based Evaluation of Cryptographic Protocol Security

17:30–17:35 Closing （Yoshihiro Mizoguchi）

18:30– Post-meeting party

[1] This conference was supported by Graduate School of Mathematics, Kyushu University, JSPS KAKENHI(Grant-in-Aid for Scientific Research (C)) Grant Number 25400217, JSPS KAKENHI(Grant-in-Aid for Scientific Research (C)) Grant Number 17K05346.

Abstract

Yota Otachi (Kumamoto University)

Title: Space-efficient algorithms for longest increasing subsequence

Abstract: Given a sequence of integers, we want to find a longest increasing subsequence of the sequence. It is known that this problem can be solved in $O(n \log n)$ time and space. Our goal in this paper is to reduce the space consumption while keeping the time complexity small. For $\sqrt{n} \leq s \leq n$, we present algorithms that use $O(s \log n)$ bits and $O(1/sn^2 \log n)$ time for computing the length of a longest increasing subsequence, and $O(1/sn^2 \log^2 n)$ time for finding an actual subsequence. We also show that the time complexity of our algorithms is optimal up to polylogarithmic factors in the framework of sequential access algorithms with the prescribed amount of space.

Yuta Watanabe (National Institute of Technology, Ube college)

Title: Association schemes on the Schubert cells of a Grassmannian

Abstract: Let $\mathbb{F}$ be any field. The Grassmannian $\mathrm{Gr}(m, n)$ is the set of m-dimensional subspaces in $\mathbb{F}^n$, and the general linear group $\mathrm{GL}_n(\mathbb{F})$ acts transitively on it. The Schubert cells of $\mathrm{Gr}(m, n)$ are the orbits of the Borel subgroup $B \subset \mathrm{GL}_n(\mathbb{F})$ on $\mathrm{Gr}(m, n)$. We consider the association scheme on each Schubert cell defined by the B-action and show it is symmetric and it is the generalized wreath product of one-class association schemes, which was introduced by R. A. Bailey in European Journal of Combinatorics 27 (2006) 428–435.

Hajime Tanaka (Tohoku University)

Title: The Terwilliger algebra with respect to an edge of a bipartite 2-homogeneous distance-regular graph

Abstract: For a bipartite Q-polynomial distance-regular graph, it follows that the Terwilliger algebra with respect to an edge behaves in a way very similar to the ordinary Terwilliger algebra with respect to a vertex. In particular, we show that the structure of the Terwilliger algebra with respect to an edge of a bipartite 2-homogeneous distance-regular graph is completely determined from the intersection array.

Akihiro Munemasa (Graduate School of Information Sciences, Tohoku University)

Title: A graph with smallest eigenvalue -3 related to the shorter Leech lattice

Abstract: We demonstrate that there exists a graph with 23 vertices having smallest eigenvalue greater than -3, such that, when represented by norm 3 vectors in a 23-dimensional Euclidean space, it generates an integral lattice L whose dual has minimum norm 3. The lattice L turns out to be a sublattice of index 2 in the shorter Leech lattice. This phenomenon can be considered as a norm 3 analogue of the fact that the Dynkin diagram of E_8 generates a unimodular lattice of minimum norm 2.

Kenichi Arai (Nagasaki University)

Title: Computer-based Evaluation of Cryptographic Protocol Security

Abstract: The complexity of cryptographic protocols has increased in recent years in response to various requirements. This increase in complexity makes the evaluation of cryptographic protocol security difficult and increases the likelihood of human error. For this reason, the problem has arisen that many studies contain evaluation errors. This study focuses on the effectiveness of computer-based evaluation of cryptographic protocol security and aims to realize a method for rigorously conducting such evaluations. In this talk, we will introduce our recent study results.