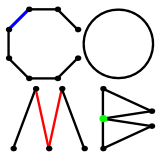

2011 年度

第 1 回 **九州大学 組合せ数学セミナー**[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（九大数理）
谷口 哲至（松江高専）
三枝崎 剛（大分高専）
アドバイザー : 坂内 英一（九大数理）

記

日時: 2011 年 4 月 23 日 (土)　13:00–17:20
場所: 九州大学伊都キャンパス 数理棟 3F 中セミナー室 7 （福岡市西区元岡 744）
URL: `http://comb.math.kyushu-u.ac.jp/`

プログラム

13:00 – 13:05 開会宣言 （谷口 哲至）

13:05 – 13:45 Xavier Dahan （九大数理）
Ramanujan graphs of very large girth based on octonions

13:55 – 14:35 Kirill Morozov （九大 IMI）
Introduction to code-based public key encryption

14:45 – 15:35 野崎 寛 （東北大情報）
グラフの埋め込みから得られる 2 距離集合について

15:45 – 16:25 栗原　大武 （東北大理）
excess とアソシエーションスキームについて

16:35 – 17:15 坂下 一生 （九大数理）
Introduction to Coq Proof Assistant System

17:15 – 17:20 総括 （溝口 佳寛）

19:00 –　懇親会

[1] このセミナーは, 九州大学大学院 数理学研究院 グローバル COE プログラム「マス・フォア・インダストリ研究教育拠点」の支援を受けて開催されます。

Abstract

Xavier Dahan（九州大学大学院 数理学研究院）

タイトル: Ramanujan graphs of very large girth based on octonions

概要: In a celebrated 1988's article, Lubotzky-Philipps-Sarnak introduced the notion of "Ramanujan graphs". They are defined as regular, undirected, connected graphs whose spectral gap reaches the Alon-Boppana's bound. These graphs had a huge impact mainly because they are then good "expander" graphs (highly connected while sparse graphs). They also hold interesting combinatorial properties: they have a large girth, a small diameter, a large chromatic number. These properties are very hard to achieve simultaneously! Indeed, since 1988, despite numerous efforts, no other construction has improved these results. We will present a new construction of Ramanujan graphs, that significantly improve these properties.
(J-P Tillich との共同研究 : arXiv:1011.2642)

Kirill Morozov（九州大学 マス・フォア・インダストリ研究所）

タイトル: Introduction to code-based public key encryption.

概要: In this talk, we will present two code-based public-key encryption (PKE) schemes: the McEliece PKE and its dual, the Niederreiter PKE. We will discuss underlying computational problems, review basic attacks, and provide some evidences why these schemes are believed to be "oneway" (OW) — a very basic and intuitive security notion. Next, we will present a simple trick which will upgrade these schemes in order to achieve "semantic security" (also known as "security against chosen plaintext attack") — another basic notion, which is believed to be a minimal requirement for security of modern PKE. This talk is targeted at a general mathematical audience.

野崎 寛（東北大学大学院 情報学研究科）

タイトル: グラフの埋め込みから得られる 2 距離集合について
(Euclidean representations of a graph as two-distance sets.)

概要: ユークリッド空間上の有限個の点の集合 X で，異なる 2 点間のユークリッド距離の集合（$A(X) = \{d(x,y)|x,y \in X, x \neq y\}$）のサイズが 2 であるものを 2 距離集合と呼んでいる。例えば，$\mathbb{R}^2$ 上の正方形の頂点集合は，辺と対角線にあたる 2 つの距離があるため，2 距離集合である。X を頂点集合とし，短い距離を持つ 2 点を辺で結べば，そこにはグラフの構造を入れることが出来る。逆に単純グラフを与えたときに，グラフの構造を持つ 2 距離集合として，何次元の空間に実現できるかが最近 Roy(2010) により示された。本講演では，グラフの 2 距離集合としての埋め込みについて，Einhorn-Schoenberg(1966), Roy(2010) などの結果を紹介し，新しい結果として，その埋め込みがいつ球面に乗るかを議論したい。さらに時間が許せば，埋め込みから得られる強正則グラフの新しい特徴づけも紹介する。
（篠原雅史氏との共同研究）

栗原 大武（東北大学大学院 理学研究科）

タイトル: excess とアソシエーションスキームについて
(On excesses and association schemes)

概要: $\Gamma = (X, E)$ を直径 d の連結な正則グラフとし，頂点 x から距離 d の位置にある点の個数を x の excess と呼び $k_d(x)$ であらわす．excess theorem とは，excess の平均値 $\frac{1}{|X|}\sum_{x\in X} k_d(x)$ が，グラフの固有値とその重複度によって決まる定数で上から抑えられ，更にその等号が成立する為の必要十分条件が，このグラフが距離正則グラフになるということである．つまり，グラフの隣接関係を用いたアソシエーションスキームの構造が入るかどうかを調べるには，グラフの excess を見ればよい．

本講演では，栗原–野崎によって得られた P 多項式スキームの同値条件を excess theorem の立場から紹介する．更に，グラフの代数的に双対な概念にあたる多項式空間に対してある不等式を与え，その不等式の等号成立と多項式空間が Q 多項式スキームになることが同値であること（つまり多項式空間に対する excess theorem）について述べる．

坂下 一生（九州大学大学院 数理学府）

タイトル: Introduction to Coq Proof Assistant System.

概要: Coq は INRIA によって開発されたコンピュータ上で数学の証明を行うソフトウェアです。この Coq は４色問題の完全な形式的証明が記述され, 検証出来ることでも知られています。今回はこの Coq を使って簡単な問題を証明と検証を行うことで基本的な使い方とその可能性をご紹介したいと思います。