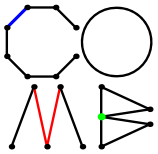
2011 年度　**九州大学**

第 9 回 **論理と計算** & 第 4 回 **組合せ数学** **合同セミナー**



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）　井口 修一（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 11 月 26 日 (土)　13:00–18:00
場所: 九州大学伊都キャンパス 数理棟 3F 大講義室 3 （福岡市西区元岡 744）
共催: 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」
URL:
（論理と計算） `http://sakura.math.kyushu-u.ac.jp/wiki/index.php?Seminar`
（組合せ数学） `http://comb.math.kyushu-u.ac.jp/`
（GCOE） `http://gcoe-mi.jp/`

プログラム

12:55 – 13:00 開会宣言 （谷口 哲至）

13:00 – Reynald Affeldt（産総研）
Instrumenting Error-correcting Codes with SSReflect

14:00 – 宗政 昭弘（東北大情報）
Super Catalan numbers and Krawtchouk polynomials

15:00 – 赤間 陽二（東北大理）
Set systems: Order types, continuous nondeterministic deformations, and quasi-orders

16:00 – 若林 徳子（九産大）
Double shuffle and Hoffman's relations for multiple L-star values

17:00 – 篠原 直行（情報通信研究機構）
Primality proving and Grantham's problem

18:00 – 18:05 総括 （溝口 佳寛）

19:30 – 懇親会

Abstract

Reynald Affeldt（産業技術総合研究所）

タイトル: Instrumenting Error-correcting Codes with SSReflect

概要: Our motivation is to provide in the Coq proof-assistant formal definitions and lemmas about error-correcting codes. The resulting toolkit could enable, for example, formal verification of implementations of cryptographic schemes based on error-correcting codes. For that purpose, we use the SSReflect library, that provides an integrated formalization of matrices and polynomials. As a technical introduction to formal verification in the Coq proof-assistant, we report on the formalization of basic properties of error-correcting codes and probabilities.

宗政 昭弘（東北大学大学院 情報科学研究科）

タイトル: Super Catalan numbers and Krawtchouk polynomials

概要: In 1992, Ira Gessel defined super Catalan number $S(m,n)$ as

$$S(m,n) = \frac{(2m)!(2n)!}{m!n!(m+n)!},$$

where m, n are positive integers, and showed that $S(m,n)$ is an integer. In this talk, we point out an interpretation of $S(m,n)$ as a special value of a Krawtchouk polynomial $K_j^d(x)$. Krawtchouk polynomials appear as the coefficients of the so-called MacWilliams identities, and also as the eigenvalues of the distance-j graph of the d-dimensional cube. Our interpretation shows that $\{(-1)^m S(m,n) \mid m, n \geq 0,\ m+n=j\}$ coincides with the set of non-zero eigenvalues of the distance-j graph of the $2j$-dimensional cube.

This is joint work with Evangelos Georgiadis and Hajime Tanaka.

赤間 陽二（東北大学大学院 理学研究科）

タイトル: Set systems: Order types, continuous nondeterministic deformations, and quasi-orders

概要: By reformulating a learning process of a set system L as a game between Teacher and Learner, we define the order type of L to be the order type of the game tree, if the tree is well-founded. The features of the order type of L (dim L in symbol) are (1) we can represent any well-quasi-order (wqo for short) by the set system L of the upper-closed sets of the wqo such that the maximal order type of the wqo is equal to dim L; (2) dim L is an upper bound of the mind-change complexity of L. dim L is defined iff L has a finite elasticity (fe for short), where, according to computational learning theory, if an indexed family of recursive languages has fe then it is learnable by an algorithm from positive data. Regarding set systems as subspaces of Cantor spaces, we prove that fe of set systems is preserved

by any continuous function which is monotone with respect to the set-inclusion. By it, we prove that finite elasticity is preserved by various (nondeterministic) language operators (Kleene-closure, shuffle-closure, union, product, intersection, ...). The monotone continuous functions represent nondeterministic computations. If a monotone continuous function has a computation tree with each node followed by at most n immediate successors and the order type of a set system L is α, then the direct image of L is a set system of order type at most n-adic diagonal Ramsey number of α. Furthermore, we provide an order-type-preserving contravariant embedding from the category of quasi-orders and finitely branching simulations between them, into the complete category of subspaces of Cantor spaces and monotone continuous functions having Girard 's linearity between them.(To appear in Theoretical Computer Science doi:10.1016/j.tcs.2011.08.010)

若林 徳子（九州産業大学 工学部 基礎教育サポートセンター）

タイトル: Double shuffle and Hoffman's relations for multiple L-star values

概要: 多重ゼータ値とは，リーマンゼータ関数の特殊値のある種の一般化である．荒川-金子は，ディリクレ指標を用いた多重ゼータ値の一般化として多重 L 値を定義した．荒川-金子によって多重 L 値の代数的定式化が導入され，一般複シャッフル関係式やホフマンの関係式の一般化である導分関係式が示された．本講演では，多重 L 値の線形和で定義される等号付き多重 L 値の代数的定式化を考え，一般複シャッフル関係式とホフマンの関係式に相当するものの導出を試みる．

篠原 直行（情報通信研究機構 ネットワークセキュリティ研究所）

タイトル: Primality proving and Grantham's problem

概要: There are two kinds of algorithms to determine the primality of a given integer. The one is a primality test which is efficient but probabilistic, namely, it rarely makes a wrong answer. Another is a primality proving that always gives a correct answer, but it is not so efficient. In this talk, we consider to construct an efficient primality proving by improving Quadratic Frobenius primality test. In order to achieve our aim, we discuss Grantham's Problem.