Practical Applications of Design Theory - Part I

(Org: **Thaís Bardini Idalino** (Universidade Federal de Santa Catarina, Brazil), **Jonathan Jedwab** (Simon Fraser University) and/et **Shuxing Li** (Simon Fraser University))

YASMEEN AKHTAR, IISER Pune, India
Level-wise Screening via Locating Arrays

A (d, t)-locating array (LA) is a covering array of strength t with the property that any set of d number of t-tuples can be distinguished from any other such set by appearing in a distinct set of rows. The number of rows in LA grows logarithmically in the number of columns, making it a cost-efficient design. We propose a screening method based on LA to identify important factors that significantly impact the response and validate our method on well-studied data sets.

This talk is based on joint work with F. Zhang, C.J. Colbourn, J. Stufken, and V.R. Syrotiuk.

LUCIA MOURA, University of Ottawa
Variable-strength arrays and applications

In this talk, we discuss variable-strength versions of covering arrays, orthogonal arrays and cover-free families. Applications include software testing, secret sharing and modification-tolerant digital signatures.

MAURA PATERSON, Birkbeck, University of London
Authentication codes with perfect secrecy and algebraic manipulation detection codes

The construction and analysis of authentication codes for providing authentication in an unconditionally secure setting is a long-standing practical application of design theory. Algebraic manipulation detection (AMD) codes were introduced by Cramer et al. in EUROCRYPT 2008 in order to apply ideas used in the construction of robust secret sharing schemes to more general cryptographic systems. In this talk we examine automorphism groups of authentication codes and show that AMD codes can be viewed as a special case of splitting authentication codes with perfect secrecy.

This talk is based on joint work with Doug Stinson.

BRETT STEVENS, Carleton University
Single change covering designs

A single change covering design (SCCD) is an ordered list of blocks with the property that every pair of consecutive blocks differ by the removal and introduction of one point. They were independently proposed twice as the solution to minimizing costs of testing and of algorithm implementations. We will discuss two applications and survey construction techniques.

DOUG STINSON, University of Waterloo
On equitably ordered splitting BIBDs

A splitting BIBD is a combinatorial design that can be used to construct splitting authentication codes with good properties. If a splitting BIBD can be equitably ordered, then the associated authentication code also provides perfect secrecy.

For various pairs $(k; c)$, we determine necessary and almost sufficient conditions for the existence of $(v; k \times c; 1)$-splitting BIBDs that can be equitably ordered. Our results cover the pairs $(k; c) = (3; 2)$; $(4; 2)$; $(3; 3)$ and $(3; 4)$, as well as all cases with $k = 2$.

This talk is based on joint work with Maura Paterson.