Algebraic and Combinatorial Approaches to Designs and Codes - Part I

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

BILL MARTIN, Worcester Polytechnic Institute, MA
Selecting resilient functions for fault-tolerant random bit generation

Random number generation in constrained environments is a challenge of increasing importance in embedded security. High-security implementations call for hundreds of random bits per clock cycle. We need both high-rate physical entropy sources and robust post-processing tools that protect against adversaries.

This talk revisits a design of Sunar, Martin and Stinson which employs phase jitter in ring oscillators as entropy source and resilient functions in order to strengthen the output entropy. How gracefully do resilient functions fail when the entropy of the source is too low? What families of orthogonal arrays provide the best resilient functions to handle side-channel attacks?

KAREN MEAGHER, University of Regina
Erdős-Ko-Rado theorems for 2-transitive groups

Two permutations are *intersecting* if there is at least one element on which the permutations agree. For any permutation group, we can ask what is the size of the largest set of intersecting permutations? If a group has the property that a point stabilizer is a largest intersecting set in the group, then we say the group has the *EKR property*. In this talk I will show that all 2-transitive groups have the EKR property, and also have a further property that partially characterizes the maximum intersecting sets in the group.

AIDAN W. MURPHY, Virginia Tech, VA
Codes from curves and repair

Classical codes with minimum distance $d \geq 3$ provide structures which support both erasure recovery and error correction. In modern settings, such as in distributed storage, it is useful to be able to accomplish these tasks with fewer symbols than classical codes necessitate. In this talk, we consider constructions of such codes using polynomials and curves over finite fields. This is joint work with Gretchen Matthews.

JINGZHOU NA, Simon Fraser University
Perfect Sequence Covering Arrays

What is a cost-efficient way to design balanced sequential testing? This minisymposium will introduce you to a combinatorial design object as a potential answer, which has a subtly balanced containment property that can be preserved by group actions. The first "special" example published by Raphael Yuster in 2019 and an efficient algorithm to search for the object introduced by Rudolf Mathon and Tran van Trung will be presented. You are invited to complete this minisymposium by playing examples together. This is joint work with Jonathan Jedwab and Shuxing Li.

ANDRIAHERIMANANA RAZAFIMAHATRATRA, University of Regina
On transitive groups that do not have the Erdős-Ko-Rado property

A family of permutations $\mathcal{F}$ of a finite transitive group $G \leq \mathrm{Sym}(\Omega)$ is *intersecting* if any two permutations in $\mathcal{F}$ agree on an element of Ω. The group G is said to have the *Erdős-Ko-Rado (EKR) property* if any intersecting family of G is of size at most $\frac{|G|}{|\Omega|}$.

In this talk, I will present some constructions of transitive groups that do not have the EKR property. My main focus will be on the transitive groups corresponding to multipartite graphs. I will also talk about a measure of how far from having the EKR property a transitive group can be.